Math 5285H: Fundamental Structures of Algebra I

HW 1 Solutions, (September 21st, 2011)

All problems from Chapter 1 of Artin's Algebra.

1.4 $\begin{bmatrix}1&2\\0&1\end{bmatrix}\begin{bmatrix}0&1&2\\1&1&3\end{bmatrix}=\begin{bmatrix}2&3&8\\1&1&3\end{bmatrix}$ and $\begin{bmatrix}2&3&8\\1&1&3\end{bmatrix}\begin{bmatrix}1\\4\\3\end{bmatrix}=\begin{bmatrix}38\\14\end{bmatrix}$. We get the same result if we multiply $\begin{bmatrix}0&1&2\\1&1&3\end{bmatrix}$ and $\begin{bmatrix}1\\4\\3\end{bmatrix}$ together first.

1.6 $\begin{bmatrix}1&a\\0&1\end{bmatrix}\begin{bmatrix}1&b\\0&1\end{bmatrix}=\begin{bmatrix}1&a+b\\0&1\end{bmatrix}$ and so $\begin{bmatrix}1&a\\0&1\end{bmatrix}^n=\begin{bmatrix}1&na\\0&1\end{bmatrix}$.

Note that one can prove the second property by induction on $n\geq 1$, but did not need to for this problem.

1.7 We claim that $\begin{bmatrix}1&1&1\\0&1&1\\0&0&1\end{bmatrix}^n=\begin{bmatrix}1&n&\binom{n+1}{2}\\0&1&n\\0&0&1\end{bmatrix}$. Note that this formula holds for $n=1$, and we compute $\begin{bmatrix}1&1&1\\0&1&1\\0&0&1\end{bmatrix}\begin{bmatrix}1&a&b\\0&1&c\\0&0&1\end{bmatrix}=\begin{bmatrix}1&a+1&b+c+1\\0&1&c+1\\0&0&1\end{bmatrix}$. Recall that $\binom{n+1}{2}=1+2+\cdots+n$. Thus

$$\begin{bmatrix}1&1&1\\0&1&1\\0&0&1\end{bmatrix}^n=\begin{bmatrix}1&1&1\\0&1&1\\0&0&1\end{bmatrix}\begin{bmatrix}1&1&1\\0&1&1\\0&0&1\end{bmatrix}^{n-1}=\begin{bmatrix}1&(n-1)+1&\binom{n}{2}+(n-1)+1\\0&1&(n-1)+1\\0&0&1\end{bmatrix}$$

by induction.

1.10 $DA=\begin{bmatrix}d_1&0&\dots&0\\0&d_2&\dots&0\\\vdots&\vdots&\ddots&0\\0&0&\dots&d_n\end{bmatrix}\begin{bmatrix}a_{11}&a_{12}&\dots&a_{1n}\\a_{21}&a_{22}&\dots&a_{2n}\\\vdots&\vdots&\ddots&\vdots\\a_{n1}&a_{n2}&\dots&a_{nn}\end{bmatrix}=\begin{bmatrix}d_1a_{11}&d_1a_{12}&\dots&d_1a_{1n}\\d_2a_{21}&d_2a_{22}&\dots&d_2a_{2n}\\\vdots&\vdots&\ddots&\vdots\\d_na_{n1}&d_na_{n2}&\dots&d_na_{nn}\end{bmatrix}$ while

$AD = \begin{bmatrix} d_1a_{11} & d_2a_{12} & \dots & d_na_{1n} \\ d_1a_{21} & d_2a_{22} & \dots & d_na_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ d_1a_{n1} & d_2a_{n2} & \dots & d_na_{nn} \end{bmatrix}$. In words, DA multiplies the ith row of A by entry d_i and AD multiplies the ith column of A.

1.11 A matrix $A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$ is upper triangular if and only if $a_{ij} = 0$ whenenver $i > j$. Recall that the product $AB = \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{bmatrix}$, where $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$. If $i > j$ then there is no k such that $i \le k$ and $k \le j$ simultaneously. Consequently, if A and B are upper triangular, then the product $a_{ik}b_{kj} = 0$ for each summand of c_{ij} when $i > j$. Thus AB is also upper triangular.

1.13 We claim that the matrix $(I - A + A^2 - A^3 + \cdots + (-A)^{k-1})$ is $(I + A)^{-1}$ when $A^k = 0$. Note that

$$(I - A + A^2 - A^3 + \cdots + (-A)^{k-1})(I + A) = I + (-1)^{k+1}A^k = I.$$

We also get $(I + A)(I - A + A^2 - A^3 + \cdots + (-A)^{k-1}) = I$, thus the inverse of $(I + A)$ is as claimed.

2.2 Let us row reduce the associated augmented matrices. One possible sequence of row reductions corresponds to multiplication on the left by the following elementary matrices: $E_1 = \begin{bmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, $E_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix}$, $E_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix}$, $E_4 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1/6 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, and $E_5 = \begin{bmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Letting $b_1 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, $b_2 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$, and $b_3 = \begin{bmatrix} 0 \\ 2 \\ 2 \end{bmatrix}$, we obtain

$$E_5E_4E_3E_2E_1[A|b_1] = \begin{bmatrix} 1 & 0 & 0 & 4/3 & 0 \\ 0 & 1 & 1/2 & -1/6 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

which has solutions given by x_3 and x_4 are anything (no pivots in those columns), $x_1 = \frac{-4}{3}x_4$ and $x_2 = \frac{-1}{2}x_3 + \frac{1}{6}x_4$. On the other hand,

$$E_5E_4E_3E_2E_1[A|b_2] = \begin{bmatrix} 1 & 0 & 0 & 4/3 & 1/3 \\ 0 & 1 & 1/2 & -1/6 & 1/3 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

which has no solutions because of the pivot in column b_2. Lastly,

$$E_5E_4E_3E_2E_1[A|b_3] = \begin{bmatrix} 1 & 0 & 0 & 4/3 & 2/3 \\ 0 & 1 & 1/2 & -1/6 & -1/3 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

which also has an infinite number of solutions given by letting x_3 and x_4 be anything, $x_1 = \frac{-4}{3}x_4 + \frac{2}{3}$ and $x_2 = \frac{-1}{2}x_3 + \frac{1}{6}x_4 - \frac{1}{3}$.

2.5 We use the formula $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ to compute $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $\begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}^{-1} = \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$. Note that the first inverse can also be calculated directly by squaring $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and the inverse of $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ also follows from problem 1.6.

We use $(ABC)^{-1} = C^{-1}B^{-1}A^{-1}$ to compute

$$\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}\right)^{-1} = \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -5 & 7 \\ 3 & -4 \end{bmatrix}.$$

2.6 A direct computation yields that $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 \\ 1 & 3 & 3 & 1 & 0 \\ 1 & 4 & 6 & 4 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ 1 & -2 & 1 & 0 & 0 \\ -1 & 3 & -3 & 1 & 0 \\ 1 & -4 & 6 & -4 & 1 \end{bmatrix} = I_5$, as does

$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ 1 & -2 & 1 & 0 & 0 \\ -1 & 3 & -3 & 1 & 0 \\ 1 & -4 & 6 & -4 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 \\ 1 & 3 & 3 & 1 & 0 \\ 1 & 4 & 6 & 4 & 1 \end{bmatrix}$. This completes the problem exhibiting the desire inverse, but still leaves open how one would obtain this result.

Since there are a family of matrices based on Pascal's triangle, we could try to compute the inverse of the 2-by-2 or 3-by-3 submatrices (starting from the upper left). This data might help us guess the pattern. We might also notice that this matrix is lower triangular and so its determinant is the product of the diagonal entries, i.e. one. Thus (see problem 6.2) its inverse would also have only integer entries. Identities from combinatorics, such as $\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$, might also help one determine the inverse here.

2.10 Recall that the systems $AX = B$ and $A'X = B'$ have the same solutions if $[A'|B']$ is the row-echelon form of the augmented matrix $[A|B]$. Thus we may assume that A' is a square matrix in row echelon form and B' is a column vector such that $A'X = B'$ has a unique solution. Then (by Prop. 1.2.13) there cannot be a pivot in column B'. We claim that A' must be the identity matrix. Otherwise, A' would have a row

of zeros and $A'X = B'$ would have *an infinite number* of solutions since there is no pivot in column B'. This contradicts the above hypotheses, hence A' is the identity and $AX = \tilde{B}$ has a unique solution for all possible column vectors $\tilde{B}$.

3.1 It is easy enough to see that $(AB)^t = B^t A^t$ and that the transpose of A^t is A again. Using these facts, we see $(BB^t)^t = (B^t)^t B^t = BB^t$. Also $(B + B^t)^t = B^t + B$. This shows that BB^t and $B + B^t$ are both symmetric, for any square matrix B. To verify that the inverse of the transpose is the transpose of the inverse, we compute

$$(A^{-1})^t A^t = (AA^{-1})^t = I^t = I \quad \text{and} \quad A^t (A^{-1})^t = (A^{-1}A)^t = I^t = I.$$

4.1 a) $(1)(3) - (i)(2-i) = 2 - 2i$, b) -2, c) $(2)(1)(2) + (0)(0)(1) + (1)(0)(0) - (2)(0)(0) - (0)(0)(2) - (1)(1)(1) = 3$, d) Diagonal $(1)(2)(3)(4) = 24$.

Note: the reason that the determinant of a lower (or upper) triangular matrix is the product of the diagonal entries is because: the identity is the only permutation matrix that is upper-triangular and hence the only nonzero contribution to the alternating sum. This can also be seen by induction from expanding about the first column, recursively.

4.3 If $n = 3$, then $\det \begin{bmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{bmatrix} = 4$. We also get $\det \begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix} = 3$, $\det [2] = 2$, so let us try to prove that $\det A_n = (n-1)$ when A_n is n-by-n. By expanding about the first row, we see that $\det A_n = 2 \det A_{n-1} - (-1) \det B_{n-1}$ where B_{n-1} is the matrix obtained by crossing out the first row and second column. The matrix B_{n-1} has only one nonzero entry in the first column, so expanding about the first column, we obtain $\det B_{n-1} = (-1) \det A_{n-2}$. Notice that we are able to recgonize this submatrix as A_{n-2} since it is obtained from A_n by crossing out the first two rows and first two columns.

Thus $\det A_n = 2 \det A_{n-1} + \det B_{n-1} = 2 \det A_{n-1} - \det A_{n-2} = 2(n-2) - (n-3) = (n-1)$, by induction.

5.1 $(12)(13)(14)(15) = (15432), (123)(234)(345) = (12)(3)(45) = (12)(45), (1234)(2345) = (12453)$, and $(12)(23)(34)(45)(51) = (1)(2345) = (2345)$.

5.3 Any permutation p is the product of transpostions, so any permutation matrix P is the product of elementary matrices E_{ij} of type 2. Any such E_{ij} is the identity matrix outside of rows i, j and columns i, j, where it looks like $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Thus E_{ij} is symmetric, i.e. $E_{ij}^t = E_{ij}$. Notice that also $E_{ij}^{-1} = E_{ij}$. This proves the result when P corresponds to a transposition. In general, write $P = E_1 \cdots E_k$. Since $P^t = E_k^t \cdots E_1^t = E_k^{-1} \cdots E_1^{-1}$, it follows that $P^t = (E_1 E_2 \cdots E_k)^{-1} = P^{-1}$.

5.4 $P = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & 0 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 1 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 & 0 \end{bmatrix}$, i.e. P_{ij} equals 1 if $j = n+1-i$ and $P_{ij} = 0$ otherwise.

Let P_n denote this permutation matrix when P is n-by-n. The sign of p is $\det P_n = 1$ if $n = 4k$ or $4k+1$ and $\det P_n = -1$ if $n = 4k+2$ or $n = 4k+3$, for integer $k \geq 0$. This can be computed inductively by expanding about the first row, noting that when n is odd, $\det P_n = \det P_{n-1}$, and when n is even, $\det P_n = -\det P_{n-1}$. The cycle decomposition is $(1,n)(2,n-1)\cdots(\frac{n}{2}-1, \frac{n}{2}+1)$ if n is even (with fixed point $p(n/2) = n/2$) and the decomposition is $(1,n)(2,n-1)\cdots(\frac{n-1}{2}, \frac{n+1}{2})$ if n is odd. Measuring the number of transpositions in these cycle decompositions also gives another way to compute the sign of p.

6.2 First, let us assume $\det A = \pm 1$. Then by the cofactor formula for the inverse, i.e. Theorem 1.6.9, we see that $A^{-1} = \pm \text{cof}(A)$ when $\det A = \pm 1$. Each entry of $\text{cof}(A)$ is up to sign a determinant of a submatrix of A, and hence is an integer since A has only integer entries.

If $\det A \neq \pm 1$, then $\det A$ either equals zero, in which case A is not invertible, or $\det A = \alpha$ with $|\alpha| > 1$. In the latter case, we then would have $\det A^{-1} = 1/\alpha$. However if we were assuming that A^{-1} had only integer entries, then by formula (1.6.4), the determinant of A^{-1} is just an alternating sum of a product of integers. This it would be impossible for $\det A^{-1}$ not to be an integer, and we get a contradiction.

M.3 To see that $\text{trace}(A+B) = \text{trace}A + \text{trace}B$, we simply note that $(a_{11}+b_{11})+(a_{22}+b_{22})+\cdots+(a_{nn}+b_{nn}) = (a_{11}+a_{22}+\cdots+a_{nn}) + (b_{11}+b_{22}+\cdots+b_{nn})$. We also observe that $\text{trace}(AB) = \sum_{k=1}^{n}(\sum_{j=1}^{n} a_{kj}b_{jk})$ by looking at the diagonal entries in the matrix multiplication formula. We can rearrange this sum as $\sum_{j=1}^{n}(\sum_{k=1}^{n} b_{jk}a_{kj})$, which equals $\text{trace}(BA)$.

Finally, we can use $\text{trace}(AB) = \text{trace}(BA)$ to show also that $\text{trace}(ABC) = \text{trace}(BAC)$. Letting $C = B^{-1}$ completes the proof.

M.7 a) We either expand about the first column, or use formula (1.6.4), to write this determinant as a sum of six terms and then note this sum equals the product $(a-b)(b-c)(c-a)$. Note that even though it looks like there are eight terms in the expansion, two of them cancel each other as $abc - abc$.

b) Let $V_n = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ t_0 & t_1 & t_2 & \dots & t_n \\ t_0^2 & t_1^2 & t_2^2 & \dots & t_n^2 \\ \vdots & \vdots & \ddots & \vdots & \\ t_0^n & t_1^n & t_2^n & \dots & t_n^n \end{bmatrix}$. We claim that $\det V_n = \prod_{0 \leq i < j \leq n}(t_j - t_i)$. We prove this by induction on n with the base cases for $n = 1$ (easy to check) and $n = 2$ (part a) already verified.

Let us first apply row reductions to turn V_n into $\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & t_1 - t_0 & t_2 - t_0 & \dots & t_n - t_0 \\ 0 & t_1^2 - t_0^2 & t_2^2 - t_0^2 & \dots & t_n^2 - t_0^2 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & t_1^n - t_0^n & t_2^n - t_0^n & \dots & t_n^n - t_0^n \end{bmatrix}$, which has the same determinant as $\begin{bmatrix} t_1 - t_0 & t_2 - t_0 & \dots & t_n - t_0 \\ t_1^2 - t_0^2 & t_2^2 - t_0^2 & \dots & t_n^2 - t_0^2 \\ \vdots & \vdots & \ddots & \vdots \\ t_1^n - t_0^n & t_2^n - t_0^n & \dots & t_n^n - t_0^n \end{bmatrix}$. We then pull the scalar $(t_1 - t_0)$ out of the first column, $(t_2 - t_0)$ out of the second column, etc. to obtain

$$\begin{aligned} \det V_n &= (t_1 - t_0)(t_2 - t_0) \cdots (t_n - t_0) \\ &\cdot \det \begin{bmatrix} 1 & 1 & \dots & 1 \\ t_1 + t_0 & t_2 + t_0 & \dots & t_n + t_0 \\ t_1^2 + t_0 t_1 + t_0^2 & t_2^2 + t_0 t_2 + t_0^2 & \dots & t_n^2 + t_0 t_n + t_0^2 \\ \vdots & \vdots & \ddots & \vdots \\ t_1^{n-1} + t_1^{n-2} t_0 + \cdots + t_0^{n-1} & t_2^{n-1} + t_2^{n-2} t_0 + \cdots + t_0^{n-1} & \dots & t_n^{n-1} + t_n^{n-2} t_0 + \cdots + t_0^{n-1} \end{bmatrix}. \end{aligned}$$

We call this second matrix V'_{n-1}. We show by using linearity of the determinant in rows that $\det V'_{n-1} = \det V_{n-1}$, where $V_{n-1} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ t_1 & t_2 & \dots & t_n \\ t_1^2 & t_2^2 & \dots & t_n^2 \\ \vdots & \ddots & \vdots & \\ t_1^{n-1} & t_2^{n-1} & \dots & t_n^{n-1} \end{bmatrix}$. By induction, $\det V_{n-1} = \prod_{1 \le i < j \le n} (t_j - t_i)$. Multiplying this result by $(t_1 - t_0)(t_2 - t_0) \cdots (t_n - t_0)$ finishes the proof.

Now showing $\det V'_{n-1} = \det V_{n-1}$ by linearity actually takes a little work. One of way of seeing this is the following set of steps:

$$\begin{aligned} \det V'_{n-1} &= \\ &\det \begin{bmatrix} 1 & 1 & \dots & 1 \\ t_1 & t_2 & \dots & t_n \\ t_1^2 + t_0 t_1 + t_0^2 & t_2^2 + t_0 t_2 + t_0^2 & \dots & t_n^2 + t_0 t_n + t_0^2 \\ \vdots & \vdots & \ddots & \vdots \\ t_1^{n-1} + t_1^{n-2} t_0 + \cdots + t_0^{n-1} & t_2^{n-1} + t_2^{n-2} t_0 + \cdots + t_0^{n-1} & \dots & t_n^{n-1} + t_n^{n-2} t_0 + \cdots + t_0^{n-1} \end{bmatrix} \\ + &\det \begin{bmatrix} 1 & 1 & \dots & 1 \\ t_0 & t_0 & \dots & t_0 \\ t_1^2 + t_0 t_1 + t_0^2 & t_2^2 + t_0 t_2 + t_0^2 & \dots & t_n^2 + t_0 t_n + t_0^2 \\ \vdots & \vdots & \ddots & \vdots \\ t_1^{n-1} + t_1^{n-2} t_0 + \cdots + t_0^{n-1} & t_2^{n-1} + t_2^{n-2} t_0 + \cdots + t_0^{n-1} & \dots & t_n^{n-1} + t_n^{n-2} t_0 + \cdots + t_0^{n-1} \end{bmatrix}, \end{aligned}$$

where this second determinant is zero since the second row is a multiple of the first. Similarly, we use linearity in the second row to reduce further:

$$\det V'_{n-1} = \det \begin{bmatrix} 1 & 1 & \dots & 1 \\ t_1 & t_2 & \dots & t_n \\ t_1^2 + t_0 t_1 & t_2^2 + t_0 t_2 & \dots & t_n^2 + t_0 t_n \\ \vdots & \vdots & \ddots & \vdots \\ t_1^{n-1} + t_1^{n-2} t_0 + \cdots + t_0^{n-1} & t_2^{n-1} + t_2^{n-2} t_0 + \cdots + t_0^{n-1} & \dots & t_n^{n-1} + t_n^{n-2} t_0 + \cdots + t_0^{n-1} \end{bmatrix} + \det \begin{bmatrix} 1 & 1 & \dots & 1 \\ t_1 & t_2 & \dots & t_n \\ t_0^2 & t_0^2 & \dots & t_0^2 \\ \vdots & \vdots & \ddots & \vdots \\ t_1^{n-1} + t_1^{n-2} t_0 + \cdots + t_0^{n-1} & t_2^{n-1} + t_2^{n-2} t_0 + \cdots + t_0^{n-1} & \dots & t_n^{n-1} + t_n^{n-2} t_0 + \cdots + t_0^{n-1} \end{bmatrix},$$

and again the second term is zero because the third row is a multiple of the first.

We then obtain

$$\det V'_{n-1} = \det \begin{bmatrix} 1 & 1 & \dots & 1 \\ t_1 & t_2 & \dots & t_n \\ t_1^2 & t_2^2 & \dots & t_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ t_1^{n-1} + t_1^{n-2} t_0 + \cdots + t_0^{n-1} & t_2^{n-1} + t_2^{n-2} t_0 + \cdots + t_0^{n-1} & \dots & t_n^{n-1} + t_n^{n-2} t_0 + \cdots + t_0^{n-1} \end{bmatrix} + \det \begin{bmatrix} 1 & 1 & \dots & 1 \\ t_1 & t_2 & \dots & t_n \\ t_0 t_1 & t_0 t_2 & \dots & t_0 t_n \\ \vdots & \vdots & \ddots & \vdots \\ t_1^{n-1} + t_1^{n-2} t_0 + \cdots + t_0^{n-1} & t_2^{n-1} + t_2^{n-2} t_0 + \cdots + t_0^{n-1} & \dots & t_n^{n-1} + t_n^{n-2} t_0 + \cdots + t_0^{n-1} \end{bmatrix},$$

and the second term is zero because the third row is a multiple of the second.

By continuing in this way, we can remove all terms divisible by t_0, eventually obtaining $\det V'_{n-1} = \det V_{n-1}$ as desired.

c) We obtain a linear system from knowing prescribed values for $P(t) = c_0 + c_1 t + \cdots + c_n t^n$ at $t_0, t_1, \dots, t_n$. (This showed up when we discussed Lagrange Interpolation at the end of Section 1.2.) The corresponding matrix for this linear system is exactly the Vandermonde matrix, V_n. From the formula we saw in (b), $\det V_n \neq 0$ when all of the t_i's are distinct. Thus V_n is invertible and the linear system has a unique solution for $[c_0, c_1, \dots, c_n]^t$.

Math 5285H: Fundamental Structures of Algebra I

HW 2 Solutions, (October 5th, 2011)

All problems from Chapter 2 of Artin's Algebra.

1.3 If map $r : \mathbb{N} \to \mathbb{N}$ was a right inverse for the shift map s, then the composition sr would send 1 to 1. However, the number 1 is not in the image of s so such a right inverse is impossible.

For any $n \in \mathbb{N}$, define the map ℓ_n by $\ell_n(i) = i - 1$ if $i \geq 2$ and $\ell_n(1) = n$. Then the composition $\ell_n s$ is the identity on $\mathbb{N}$. Thus we have exhibited an infinite number of left inverses.

2.1 Group multiplication table for $S_3 = \{e, (12), (13), (23), (123), (132)\}$ with first row (resp. column) corresponding to left (resp. right-) multiplication by identity e:

	e	(12)	(23)	(13)	(123)	(132)
(12)	e	(123)	(132)	(23)	(13)
(23)	(132)	e	(123)	(13)	(12)
(13)	(123)	(132)	e	(12)	(23)
(123)	(13)	(12)	(23)	(132)	e
(132)	(23)	(13)	(12)	e	(123)

.

2.2 Let S' be the subset of S consisting of invertible elements. We must show that the associative law of composition, $\circ$, on S restricts to a law of composition on S'. In other words, we need to show **closure**: if s_1 and s_2 are invertible (i.e. in S'), then $s_1 \circ s_2$ is also invertible (i.e. in S'). But this is clearly true since $s_2^{-1} \circ s_1^{-1}$ is the inverse of $s_1 \circ s_2$. This law of composition on S' is associative since it is associative on S.

To complete the proof that subset S' is a group, we need to check that *identity* and *inverses* are in S', and these follow quickly.

2.4 a) Yes, $GL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{C})$, clearly the product of two invertible matrices with real entries is an invertible matrix with real entries (implies *closure*). The *identity* matrix has real entries, and the *inverse* of a matrix with real entries also has real entries.

b) Yes, $\{-1, 1\}$ is a subgroup of $\mathbb{R}^\times$. (Similar technique as in part (a).)

c) No, the inverse of a positive integer (under addition) is not a positive integer.

d) Yes, {positive reals} is a subgroup of $\mathbb{R}^\times$. (Similar technique as in part (a).)

e) No, matrix $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ is not invertible.

3.1 $gcd(123, 321) = 3$ since

$$\begin{aligned} 321 &= 2 \cdot 123 + 75 \\ 123 &= 1 \cdot 75 + 48 \\ 75 &= 1 \cdot 48 + 27 \\ 48 &= 1 \cdot 27 + 21 \\ 27 &= 1 \cdot 21 + 6 \\ 21 &= 3 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

We now want to express

$$3 = r \cdot 123 + s \cdot 321.$$

We use

$$3 = 1 \cdot 21 - 3 \cdot 6$$

(from the second to last line). We then plug in $6 = 1 \cdot 27 - 1 \cdot 21$, treating 6, 21, and 27 like variables:

$$3 = 4 \cdot 21 - 3 \cdot 27.$$

Continuing in this way: we see $3 = 4 \cdot 48 - 7 \cdot 27$, $3 = 11 \cdot 48 - 7 \cdot 75$, etc, and $3 = 47 \cdot 123 - 18 \cdot 321$.

3.2 Let $d = gcd(a, b)$. If $a + b = p$, then $p \in d\mathbb{Z}$ ($a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ by definition of gcd). Thus $gcd(a, b)$ divides p. But, if p is prime, then $gcd(a, b)$ is either 1 or p. However, since a and b are both positive, a and b are both less than p (by assumption $a + b = p$), hence $gcd(a, b)$ can't be p. We conclude $gcd(a, b) = 1$.

4.1 Since $a^3b = ba^3$, we also see $a^3ba^{-3} = b$. By repeatedly conjugating $a^{3k}ba^{-3k}$ for any integer k also equals b. By letting $k = 5$, $a^{15} = a$ since $a^7 = 1$. Thus, $aba^{-1} = a$ and $ab = ba$.

4.3 Assume that ab has a finite order n. Then $(ab)^n = abab \cdots ab = 1$. Multiplying on the right by a, we get $(abab \cdots ab)a = a(baba \cdots ba) = a(ba)^n = a$. Thus by the cancellation law, $(ba)^n = 1$. If $(ba)^m = 1$ for $0 < m < n$, then by similar logic, we get that $(ab)^m = 1$. However, since the *order* of ab is n, there is no m between 0 and n such that $(ab)^m = 1$. Hence ba has the same order as ab. Analogously, if ab had infinite order, then so does ba as well, and vice-versa.

4.6 a) Let $G \cong C_6$ be presented as $\{1, x, x^2, \ldots, x^5\}$ with $x^6 = 1$. *Two* of its elements, x^1 and x^5 generate G.

For C_5, any non-identity (four of its elements) generate C_5. For C_8, four of its elements, $\{x^1, x^3, x^5, x^7\}$, generate C_8.

Note: we can also think of these cyclic groups as $\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$. In this notation, the generators are $\{\overline{1}, \overline{5}\}$ for C_6, $\{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ for C_5, and $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ for C_8.

b) In general, x_i (equivalently $\overline{i}$) generates C_n if and only if $gcd(i,n) = 1$. In words, n and i are relatively prime.

You were not asked to count the number of such possible generators for the problem, but it is a basic definition from number theory that the *Euler Phi Function* $\phi(n)$ counts the number of $i \in \{1, 2, \ldots, n-1\}$ such that $gcd(i,n) = 1$.

4.7 To prove that $H = \{1, x, y, xy\}$ is a subgroup, we note that (i) the identity $1 \in H$, (ii) inverse $x^{-1} = x \in H$ since $x^2 = 1$, and same for $y^{-1} = y \in H$ and $(xy)^{-1} = xy \in H$. The element $1 = xyxy = xyx^{-1}y^{-1}$ since $x^2 = 1$, $y^2 = 1$, and $(xy)^2 = 1$ by assumption. Thus $xy = yx$, so we can conclude that (iii) H is closed under multiplication.

4.8 a) We have seen previously that any invertible matrix (with real entries), i.e. an element of $GL_n(\mathbb{R})$, is the multiplication of elementary matrices. Thus, to show that elementary matrices of the first kind and third kind generate $GL_n(\mathbb{R})$, it suffices to show that elementary matrices of the second kind (corresponding to transpositions) can be obtained by multiplying only matrices of the first and third kinds together.

$$\begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}.$$

Note that this product agrees with the sequence of row reductions in equation (1.4.12). If we have another elementary matrix of type 2 corresponding to another transposition, we use analogous matrices in the above product.

b) First, note that any elementary matrix of the first type has determinant equal to one, and thus is in $SL_n(\mathbb{R})$. As hinted, we start with the $SL_2(\mathbb{R})$ case. Observe the following equations involving products of elementary matrices of the first type:

$$\begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -1/c & 1 \end{bmatrix} \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & c \\ -1/c & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & c \\ -1/c & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} c & 0 \\ 0 & 1/c \end{bmatrix}.$$

Thus, by letting c be the appropriate nonzero real number, we can obtain any product of elementary matrices of the third type that has *det* equal to one. Letting $c = \pm 1$, we can also obtain (from the first equation) the product of a matrix of the second type and third type which each have determinant -1.

For the $n \geq 3$ case, we also have products in $SL_n(\mathbb{R})$ which are a product of an even number of elementary

matrices of the second type: e.g.

$$\begin{bmatrix}0&-1&0\\1&0&0\\0&0&1\end{bmatrix}\begin{bmatrix}1&0&0\\0&0&-1\\0&1&0\end{bmatrix}=\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}=\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}\begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix},$$

or we combine products of matrices of the third type, obtained as above, to get any matrix

$$\begin{bmatrix}d_1&0&0&0\\0&d_2&0&0\\0&0&d_3&0\\0&0&0&d_4\end{bmatrix}=\begin{bmatrix}d_1&0&0&0\\0&1/d_1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&d_1d_2&0&0\\0&0&1/d_1d_2&0\\0&0&0&1\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&d_1d_2d_3&0\\0&0&0&1/d_1d_2d_3\end{bmatrix}$$

such that $d_1d_2d_3d_4=1$. Same technique works for any $n\geq 3$.

4.9 The elements of order 2 in S_4 are the transpositions: $\{(12),(13),(14),(23),(24),(34)\}$ and the product of two disjoint transpositions: $\{(12)(34),(13)(24),(14)(23)\}$. Thus there are *nine* elements of order 2 in S_4.

Recall that any element of S_n can be written as the product of disjoint cycles, and one can observe that any other non-identity element of S_4 would contain a cycle of size larger than 1 or 2 and thus would not be an element of order two.

5.2 Firstly, assume that K and H are subgroups of G, and consider elements $m_1,m_2\in K\cap H$, i.e. in the intersection. The product $m_1m_2\in H$ since $m_1,m_2\in H$ and H is a subgroup. Similarly, $m_1m_2\in K$. Thus $m_1m_2\in K\cap H$, thus $K\cap H$ is closed under products.

The identity of G is in both K and H (thus $K\cap H$) and if $m\in K\cap H$, $m^{-1}\in K\cap H$ for similar reasons. This concludes that $K\cap H$ is a subgroup of G.

Secondly, to see that $K\cap H$ is a normal subgroup in H when K is a normal subgroup of G, we note: (i) if $m\in K\cap H$ and $h\in H$, then $hmh^{-1}\in K$ since K is normal in H. (ii) $hmh^{-1}\in H$ as well. Thus $hmh^{-1}\in K\cap H$.

5.3 $\psi\left(\begin{bmatrix}a&b\\0&d\end{bmatrix}\begin{bmatrix}e&f\\0&h\end{bmatrix}\right)=\psi\left(\begin{bmatrix}ae&af+bh\\0&dh\end{bmatrix}\right)=a^2e^2$ and $\psi\left(\begin{bmatrix}a&b\\0&d\end{bmatrix}\right)\cdot\psi\left(\begin{bmatrix}e&f\\0&h\end{bmatrix}\right)=a^2\cdot e^2$, thus ψ is a homomorphism.

Its kernel are the matrices where $a^2=1$, the identity of $\mathbb{R}^\times$. So in particular, the kernel is the subgroup of those matrices of the form $\begin{bmatrix}\pm1&b\\0&d\end{bmatrix}$. Its image is the subgroup of positive integers. (Note: $a\neq 0$ since $\begin{bmatrix}a&b\\0&d\end{bmatrix}$ is not invertible otherwise.)

5.6 We claim the *center* of $GL_n(\mathbb{R})$ is the set of matrices of the form $d\cdot I_n$ with $d\in\mathbb{R}^\times$.

To prove this, we note that any element of $GL_n(\mathbb{R})$ can be expressed as a product of elementary matrices of type 1 or 3 (Exercise 4.8a). Recall that matrix A is in the center if and only if $AB=BA$ for all

$B \in GL_n(\mathbb{R})$. Equivalently, A is in the center if and only if $BAB^{-1} = A$ for every $B \in GL_n(\mathbb{R})$. It is enough to determine the matrices A such that $BAB^{-1} = A$ for any elementary matrix B of type 1 or 3. For example, if B is the elementary matrix of type 3 $B = \begin{bmatrix} c & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}$ then the result BAB^{-1} is the matrix obtained by multiplying the first row of A by c and the first column of A by $1/c$. Consequently, if A contains some non-zero off-diagonal entry then there exists an elementary matrix of type 3 so that $BAB^{-1} \neq A$. Thus we can consider only diagonal matrices. We then consider an elementary matrix of type 1, and similarly show that there exists a B so that $BAB^{-1} \neq A$ unless all diagonal entries are equal to one-another.

Going the other direction, it is easy to verify that $BAB^{-1} = A$ whenever $A = d \cdot I_n$.

6.2 A homomorphism ψ from $\mathbb{Z}^+$ to $\mathbb{Z}^+$ must send the identity 0 to 0 and is uniquely determined by the value of $\psi(1) = n$. This is because, if $\psi(1) = n$, then

$$\psi(k) = \psi(1 + 1 + \cdots + 1) = n + n + \cdots + n = kn.$$

Since $\psi(1)$ can be any integer, there is as many homomorphisms ψ as integers. The homomorphism ψ is injective as long as $\psi(1) \neq 0$, and is surjective (hence an isomorphism) if $\psi(1) = \pm 1$.

6.3 Note that $f^2 = f \circ f$ is the identity map and $g^2 = g \circ g = \frac{\frac{x-1}{x}-1}{\frac{x-1}{x}} = \frac{-1}{x-1}$. Repeating this process, we see that g^3 is also the identity. Also the composition $f \circ g = \frac{x}{x-1}$, and $g^2 \circ f = \frac{-1}{\frac{1}{x}-1} = f \circ g$. Thus, thinking of S_3 as generated by $x = (123)$ with $x^3 = 1$ and $y = (12)$ with $y^2 = 1$, satisfying $yx = x^2y$, we get an isomorphism φ from $\langle f, g \rangle = \{id, g, g^2, f, g \circ f, g^2 \circ f\}$ to $S_3 = \{1, x, x^2, y, xy, x^2y\}$ by $\varphi(f) = y$ and $\varphi(g) = x$. Note that since we have defined φ on the generators of $\langle f, g \rangle$, we extend it to a unique homomorphism by mandating $\varphi(g^n \circ f^m) = x^n y^m$. This map is also clearly bijective with canonical inverse sending x to g and f to y.

6.6 Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{R})$. If $A \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} A^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, then it is easy to see that we must have the equations

$$\begin{aligned} ad + bd - bc &= ad - bc \\ -b^2 &= 0 \\ -c^2 &= ad - bc \\ -bc - bd + ad &= ad - bc \end{aligned}$$

These simplify to $ad = ad$, $-c^2 = ad$, $ad = ad$ after letting $b = 0$. Thus in $GL_2(\mathbb{R})$, the two elements are conjugate, in fact we just need A to be any matrix of the form $\begin{bmatrix} -c^2/d & 0 \\ c & d \end{bmatrix}$. However, such a matrix necessarily has a negative determinant, thus the two elements are *not* conjugate in $SL_2(\mathbb{R})$.

6.7 First we prove closure: if gh_1g^{-1} and gh_2g^{-1} in gHg^{-1}, then their product is $gh_1h_2g^{-1}$ which is in gHg^{-1} since H is a subgroup, hence closed under multiplication.

Secondly, H is a subgroup, so it contains the identity, and $g \cdot 1 \cdot g^{-1} = 1$ so gHg^{-1} also contains the identity.

Lastly, H is a subgroup, so for any $h \in H$, $h^{-1} \in H$. Notice that $ghg^{-1} \cdot gh^{-1}g^{-1} = 1$, and thus gHg^{-1} contains inverses.

6.10 a) As discussed in class, a homomorphism φ of a cyclic group $\{1, x^1, x^2, \ldots, x^9\}$ is completely determined by the value $\varphi(x^1)$. Such a homomorphism is bijective if and only if $\varphi(x^1) = x^1, x^3, x^7$, or x^9. These are the automorphisms of C_{10}.

b) The symmetric group S_3 is generated by $x = (123)$ and $y = (12)$. Thus a homomorphism φ is determined by where it sends x and y. If such a homomorphism is bijective, it must send an element of order 2 to an element of order 2 and an element of order 3 to an element of order 3.

Thus the possibile automorphisms are

$$\begin{aligned}
\varphi_1 &: (12) \mapsto (12), \quad (123) \mapsto (123) \\
\varphi_2 &: (12) \mapsto (12), \quad (123) \mapsto (132) \\
\varphi_3 &: (12) \mapsto (13), \quad (123) \mapsto (123) \\
\varphi_4 &: (12) \mapsto (13), \quad (123) \mapsto (132) \\
\varphi_5 &: (12) \mapsto (23), \quad (123) \mapsto (123) \\
\varphi_6 &: (12) \mapsto (23), \quad (123) \mapsto (132).
\end{aligned}$$

It is easy to verify that all six of these maps are in fact isomorphisms.

Note: one can easily compute that φ_1 is the identity automorphism (conjugation by 1), φ_2 agrees with conjugation by (12), φ_3 agrees with conjugation by (132), φ_4 agrees with conjugation by (23), φ_5 agrees with conjugation by (123), and φ_6 agrees with conjugation by (13).

Remark: the automorphism that can be obtained by conjugation are known as *inner automorphisms*. We have just shown that all automorphisms of S_3 are *inner*. This will come up again in Chapter 6.

Math 5285H: Fundamental Structures of Algebra I

HW 3 Solutions, (October 26th, 2011)

Problems from Chapter 3 of Artin's Algebra:

1.2 To find the inverse of 5 modulo p, we wish to solve the congruence $5x \equiv 1 \mod p$. This is equivalent to solving the equation

$$5x + pk = 1$$

for integers $x \in \{0, 1, 2, \ldots, p-1\}$ and $k \in \mathbb{Z}$.

For $p = 7$, we want to solve $5x + 7k = 1$. Using the Euclidean algorithm, we see

$$7 = 1 \cdot 5 + 1 \cdot 2 \quad \text{and} \quad 5 = 1 \cdot 2 \cdot 2 + 1.$$

Consequently,

$$1 = 1 \cdot 5 - 2 \cdot 2$$

and

$$1 = 1 \cdot 5 - 2(7 - 5) = 3 \cdot 5 - 2 \cdot 7.$$

Thus we conclude that $5 \cdot 3 = 15 \equiv 1 \mod 7$. Note that we could also get this by trial and error, but in general the Euclidean algorithm method will be quicker for large p. By a similar method, we obtain

$$5 \cdot 9 \equiv 1 \mod 11, \quad 5 \cdot 8 \equiv 1 \mod 13, \quad \text{and} \quad 5 \cdot 7 \equiv 1 \mod 17.$$

Let us illustrate the Euclidean algorithm also for 17: $17 = 3 \cdot 5 + 2$, $5 = 2 \cdot 2 + 1$, thus

$$1 = 1 \cdot 5 - 2 \cdot 2 = 1 \cdot 5 - 2 \cdot (1 \cdot 17 - 3 \cdot 5) = 7 \cdot 5 - 2 \cdot 17.$$

1.5 Over a general field, e.g. $\mathbb{F}_p$, we still have that A is invertible if and only if $\det A \neq 0$, as an element of the field.

$$\begin{aligned}\det A &= \det \begin{bmatrix} 1 & 2 & 0 \\ 0 & 3 & -1 \\ -2 & 0 & 2 \end{bmatrix} \\ &= (1)(3)(2) + (2)(-1)(-2) + (0)(0)(0) - (1)(-1)(0) - (2)(0)(2) - (0)(3)(-2) \\ &= \overline{10} \mod p.\end{aligned}$$

Thus A is invertible as long as p is not 2 nor 5.

Not needed for the proof but: for example, over $\mathbb{F}_2$, we see A becomes $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$, which has a row of zeros. Over $\mathbb{F}_5$, A becomes $\begin{bmatrix} 1 & 2 & 0 \\ 0 & 3 & 4 \\ 3 & 0 & 2 \end{bmatrix}$, and we have a non-trivial linear combination (in $\mathbb{F}_5$) of columns:

$$1 \cdot \begin{bmatrix} 1 \\ 0 \\ 3 \end{bmatrix} + 2 \cdot \begin{bmatrix} 2 \\ 3 \\ 0 \end{bmatrix} + 1 \cdot \begin{bmatrix} 0 \\ 4 \\ 2 \end{bmatrix} = \begin{bmatrix} 5 \\ 10 \\ 5 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \mod 5.$$

1.6 a) We row reduce $\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$ over $\mathbb{Q}$ to obtain

$$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & -1 & 1 & -2 \\ 0 & -2 & -1 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & -1 & 2 \\ 0 & -2 & -1 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 1 & -1 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & -3 & 4 \end{bmatrix}$$

Thus far, we have only added multiples of one row to another or multiplied the second row by (-1).

Next, we *divide* the third row by -3 and then clear the entries in the rest of the third column to get

$$\begin{bmatrix} 1 & 0 & 1 & -1 \\ 0 & 1 & -1 & 2 \\ 0 & 0 & 1 & -4/3 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 & 1/3 \\ 0 & 1 & 0 & 2/3 \\ 0 & 0 & 1 & -4/3 \end{bmatrix}.$$

Thus, over $\mathbb{Q}$, the unique solution to $AX = B$ is $X = \begin{bmatrix} 1/3 \\ 2/3 \\ -4/3 \end{bmatrix}$.

(b) and (d): we can do a similar technique. Dividing by 3 in $\mathbb{F}_2$ is equivalent to dividing by 1, which means multiplying by 1's multiplicative inverse, which is 1. Thus we get $X = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ over $\mathbb{F}_2$.

Dividing by 3 in $\mathbb{F}_7$ is equivalent to multiplying by 3's multiplicative inverse, which is 5 since $3 \cdot 5 = 15 \equiv 1 \mod 7$. Thus we get $X = \begin{bmatrix} 1 \cdot 5 \\ 2 \cdot 5 \\ -4 \cdot 5 \end{bmatrix} \equiv \begin{bmatrix} 5 \\ 3 \\ 1 \end{bmatrix}$ over $\mathbb{F}_7$. (More precisely, when row-reducing, instead of dividing by (-3), we would multiply by (-5) and continue row-reducing from there the same way.)

c) Since we cannot divide by -3 in $\mathbb{F}_3$, we go back to row-reducing step by step.

$$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 2 & 1 & 1 \\ 0 & 1 & 2 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 1 & 2 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

At this point, we have a row of zeros followed by a (non-zero) pivot in the column corresponding to B. Thus there are no solutions $AX = B$ in $\mathbb{F}_3$.

1.8 a) Here p is a prime integer.

Answer 1: Since we know that $\mathbb{F}_p^\times$ is a multiplicative group of order $(p-1)$, we know that $\overline{a}^{p-1} = \overline{1}$ for all $\overline{a} \in \mathbb{F}_p^\times$. Multiplying through by $\overline{a}$, we have the identity $\overline{a}^p = \overline{a}$ for all $\overline{a} \in \mathbb{F}_p^\times$ Consequently, we have that for any integer a with $a \not\equiv 0 \mod p$, then $a^p = a + kp$ for some k, i.e. $a^p \equiv a \mod p$.

Now, if $a \equiv 0 \mod p$, i.e. is a multiple of p, then, $a^k \equiv a \mod p$ (follows from $\overline{0}^k = \overline{0}$) for any power k, including $k = p$. Thus we have the identity for all integers a.

Answer 2: Consider

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + 1.$$

We first note that $\binom{p}{k} = \frac{p!}{k!(p-k)!} \equiv 0 \mod p$ unless $k = 0$ or p. This is because, in those cases, the denominator is the product of a subset of numbers between 1 and $p-1$ and only the numerator contains a factor of p. Thus $(a+1)^p \equiv a^p + 1 \mod p$, and we can prove that $a^p \equiv a \mod p$ for all nonnegative integers a by induction. (Start with the base case $0^p = 0$.) The proof for negative integers can be proven using $(a-1)^p \equiv a^p + (-1)^p \equiv a^p - 1 \mod p$.

b) For every $\overline{a} \in \mathbb{F}_p^\times$, there exists a unique $\overline{a^{-1}} = \overline{a}^{-1}$. Furthermore, we have that $\overline{a^{-1}} = \overline{a}$ if and only if $\overline{a}^2 = 1$, i.e. if and only if $\overline{a} = \overline{1}$ or $\overline{p-1}$. Thus with these two exceptions, in the product $(p-1)! \equiv (\overline{p-1})(\overline{p-2}) \cdots (\overline{2})(\overline{1}) \mod p$, we have cancellation in pairs until we are left with $(p-1)! \equiv (\overline{p-1})(\overline{1}) \equiv -1 \mod p$.

Note that, technically the above argument only works if $p > 2$, but if $p = 2$ then $-1 \equiv 1 \mod p$ and it is easy to see that $(p-1)! = 1$.

1.9 Recall that $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$. Thus, the order of A is p in $GL_2(\mathbb{F}_p)$ (in particular 7 in $GL_2(\mathbb{F}_7)$).

$B = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 2^n & 0 \\ 0 & 1 \end{bmatrix}$, and so the order of B in $GL_2(\mathbb{F}_p)$ is equivalent to the multiplicative order of 2 modulo p. Thus, in particular, modulo 7, the order is 3 since $2^3 = 8 \equiv 1 \mod 7$.

1.10 We must show that the three field axioms (Definition 3.2.2) are satisfied:

I.e. with matrix entries in $\mathbb{F}_2 = \{0, 1\}$,

(i) Addition makes $F = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right\}$ into an abelian group.

(ii) Multiplication is commutative and it makes the set $F^\times = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\}$ into an abelian group.

(iii) The distributive law $a(b + c) = ab + ac$.

Note that we can use that modular arithmetic is well-defined and that matrix-addition and -multiplication are both associative and satisfy the distributive law. It is also clear that the usual additive identity and multiplicative identity are in F and $F^\times$, respectively. We also see that matrix-addition is commutative.

Thus it suffices to show that F is closed under addition and additive inverses and that $F^\times$ is closed under multiplication and multiplicative inverses.

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \equiv \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \quad \text{and} \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Commutativity of addition shows the remaining necessary sums are in $\mathbb{F}$. Furthermore, every element is its own additive inverse since we are working over $\mathbb{F}_2$.

We make a similar table for multiplication:

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \equiv \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \text{ and } \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

thus concluding that $\mathbb{F}^\times$ is multipicatively closed, commutative, and contains inverses.

1.11 Analogous to problem 1.10, we know that usual addition and multiplication over the complex numbers is commutative, associative, and distributive, so we do not need to verify any of these when working $\{a + bi : a, b \in \mathbb{F}_p\}$.

$F = \{a+bi : a, b \in \mathbb{F}_p\}$ which is clearly closed under addition and multiplication and contains p^2 elements. Further, $a + bi$ has additive inverse $-a - bi$ where we consider $-a$ and $-b$ modulo p. The only nontrivial item to check is that any nonzero $a + bi$ has a multiplicative inverse in F.

We now consider $p = 3$: in this case $1 + 0i$ is the identity and $2 + 0i$ has itself as its inverse. $0 + i$ and $0 + 2i$ are each other's inverses (since $i \cdot 2i = -2 \equiv 1 \mod 3$). $1 + i$ and $2 + i$ are each other's inverse

$((1+i)(2+i) = 2+2i+i+(-1) \equiv 1+0i \mod 3)$, and $1+2i$ has inverse $2+2i$ as $(1+2i)(2+2i) = 2+4i+2i+(-4) \equiv 1+0i \mod 3)$.

Note we could also use the general rule $(a+bi)^{-1} = (a^2+b^2)^{-1}(a-bi) \equiv (a^2+b^2)^{-1}(a+2bi)$ whenever $a^2+b^2 \not\equiv 0$. But, in particular $1^2 \equiv 2^2 \equiv 1$ so if only one out of a or b are nonzero then $(a^2+b^2) \equiv 1$ and if both are nonzero then $(a^2+b^2) \equiv 2$. So in $\mathbb{F}_3$, we can never have $a^2+b^2 \equiv 0$ unless both a and $b \equiv 0$, hence why all of these inverses are defined. Note that this also implies that multiplication is closed in $F^\times$ as well since if $(a+bi)(c+di) \equiv (0+0i)$ we could multiply both sides by $(a+bi)^{-1}$ and get a contradiction.

We now try to do the same strategy for $p = 5$. Note that in this case, that if we (for example) let $a = 1$ and $b = 2$, then $a^2+b^2 \equiv 0 \mod 5$ even though $1+2i \not\equiv 0+0i$. Thus if we try to invert $1+2i$ we will run into a problem:

$$(1+2i)(a+bi) = (a-2b)+(2a+b)i \equiv (a+3b)+(2a+b)i$$

and we want to solve the matrix equation $\begin{bmatrix}1 & 3\\ 2 & 1\end{bmatrix}\begin{bmatrix}a\\ b\end{bmatrix} = \begin{bmatrix}1\\ 0\end{bmatrix}$ over $\mathbb{F}_5$. However the determinant of this matrix is $-5 \equiv 0 \mod 5$ and in particular the second row is actually twice the first one. Thus one can see that this system has no such solution.

Another manifestation of this problem is that $(1+2i)(1+3i) = -5+5i \equiv 0+0i$ which is not actually in $F^\times$. So while multiplication over F is closed, it is not closed in $F^\times$ in this case. Note that choosing $1+2i$ was a little arbitrary, there are other choices of a and b such that $a+bi$ is also not invertible over $\mathbb{F}_5$.

Now let us consider $p = 7$. In this case, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 2$, $4^2 \equiv 4$, $5^2 \equiv 4$ and $6^2 \equiv 1$. Clearly for nonzero a, $a+0i$ has $a^{-1}+0i$ as its inverse and for nonzero b, $0+bi$ has $0-b^{-1}i$ as its inverse, where a^{-1} and b^{-1} signify the inverse in $\mathbb{F}_7^\times$. But if we consider $a+bi$, where a and b are both nonzero (i.e. in $\mathbb{F}_7^\times$), then by the above a^2+b^2 is a sum of two of the three numbers from $\{1,2,4\}$. No such sum can be congruent to 0 modulo 7. Thus all nonzero $a+bi$ in F have a multiplicative inverse when working over $\mathbb{F}_7$ using the formula $(a+bi)^{-1} = (a^2+b^2)^{-1}(a-bi) \equiv (a^2+b^2)^{-1}(a+6bi)$.

Answer 2: An alternative way of seeing what goes right in the cases $\mathbb{F}_3$ and $\mathbb{F}_7$, but goes wrong in $\mathbb{F}_5$ is the definition of $i = \sqrt{-1}$.

In $\mathbb{F}_3$, $-1 \equiv 2$ and there is no $a \in \mathbb{F}_3$ such that $a^2 \equiv 2 \mod 3$. Similarly, there is no $a \in \mathbb{F}_7$ such that $a^2 \equiv 6 \mod 7$, as we saw above. Thus in these cases, we can extend the field $\mathbb{F}_p$ by adjoining a new symbol representing this square root of negative one.

However, in $\mathbb{F}_5$, $-1 \equiv 4 \equiv 2^2 \equiv 3^2$ and so in some sense the symbol i is the same as the symbol 2 or $3 \in \mathbb{F}_5$. So in a vague sense, $1+2i \equiv 1+2(2) \equiv 5 \equiv 0$ and so it is not surprising that such an element is not invertible and that we can find an element, $1+3i \equiv 1+3(3) \equiv 10 \equiv 0$, to multiply it by to get zero.

We will make this vague sense more precise later in the course. The idea is that $1+2i$ and $1+3i$ are what would be called *zero divisors* of the *ring* consisting of $\{a+bi : a,b \in \mathbb{F}_5\}$.

3.1 We claim that the set $\{E_{ii}\}_{i=1..n} \cup \{E_{ij} + E_{ji}\}_{i=1..n, j=1..n, i \neq j}$ is a basis for the set of symmetric matrices. Here, E_{ij} denotes the matrix with a 1 in the (i,j)th entry and 0's everywhere else.

It is clear to see that each of these matrices are indeed symmetric. Secondly, they span any symmetric matrix since if $A^t = A$, we must have that the off-diagonal entry (i,j) agrees with the entry (j,i). Thus, considering the entries in the lower triangle of the matrix (i.e. $i \geq j$ we can write any symmetric matrix as a linear combination of the above entries.

Lastly, this set of matrices is independent since the set $\{E_{ij}\}_{i=1..n, j=1..n}$ is independent for the space of all $n \times n$ matrices and each of the matrices in the proposed basis contain disjoint indexes.

3.2 We row reduce the matrix A to obtain

$$\begin{bmatrix} 2 & 1 & 2 & 3 \\ 1 & 1 & 3 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 1/2 & 1 & 3/2 \\ 0 & 1/2 & 2 & -3/2 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & -1 & 3 \\ 0 & 1 & 4 & -3 \end{bmatrix}.$$

Considering the non-pivot columns, let $x_3 = 1$ and $x_4 = 0$ and we get $x_1 - (1) + 3(0) = 0$, hence $x_1 = 1$ and $x_2 + 4(1) - 3(0) = 0$, hence $x_2 = -4$.

Thus the vector $\begin{bmatrix} 1 \\ -4 \\ 1 \\ 0 \end{bmatrix}$ is in the nullspace W. We also can let $x_3 = 0$ and $x_4 = 1$ (ensures independence from the previous vector), and obtain vector $\begin{bmatrix} -3 \\ 3 \\ 0 \\ 1 \end{bmatrix}$. Putting these two vectors together gives us a basis for W.

Note: We can pick any other set of linearly independent vectors in $\mathbb{R}^2$ as our two choices for non-pivot columns x_3 and x_4 to get a different basis for W. This choice of basis is far from unique.

4.3 We saw in class, e.g. Proposition 3.5.9, that we can get from one basis $\mathbf{B}$ to another by multiplying by an invertible matrix P. Furthermore, we know that any invertible matrix can be written as the product of elementary matrices, E_i. Lastly, if we multiply $E_i\mathbf{B} = \mathbf{B}'$, the resulting basis $\mathbf{B}'$ is obtained from $\mathbf{B}$ by one of these three types of transformations. Whether it is transformation (i), (ii), or (iii) just depends on whether E_i is an elementary matrix of type 1, 3, or 2.

4.4 a) To obtain a basis for $V = \mathbb{F}_p^2$, we must first pick a nonzero vector $v_1 \in V$ and secondly pick $v_2 \in V$ that is not a scalar multiple of v_1. Comparing this procedure with picking a matrix M in $GL_2(\mathbb{F}_p)$, we note that we must pick a nonzero first column v_1. And to ensure invertibility of M, the second column cannot be a multiple of v_1. Since these two procedures are the same, it follows that the number of bases in V equals the number of matrices in $GL_2(\mathbb{F}_p)$.

b) Using the procedure described in (a), the number of matrices in $GL_2(\mathbb{F}_p)$ is $(p^2-1)(p^2-p)$, where p^2-1 is the number of nonzero vectors v_1 in V and p^2-p is the number of vectors $v_2 \in V$ that are not multiples of v_1. (There are p such multiples since $|\mathbb{F}_p| = p$.) We factor $(p^2-1)(p^2-p) = (p-1)^2(p+1)p$ to get the desired form.

Consider the surjective map $\det : GL_2(\mathbb{F}_p) \to \mathbb{F}_p^\times$ with kernel equal to $SL_2(\mathbb{F}_p)$. Since the image of det has cardinality $(p-1)$, it follows that $SL_2(\mathbb{F}_p)$ is an index $(p-1)$ subgroup of $GL_2(\mathbb{F}_p)$ and that $|SL_2(\mathbb{F}_p)| = |GL_2(\mathbb{F}_p)|/(p-1) = (p-1)(p+1)p$.

Answer 2 for $SL_2(\mathbb{F}_p)$: To get a matrix M in $SL_2(\mathbb{F}_p)$ instead, we start with the same procedure, but when we choose v_2, we can also pick λv_2 instead, and the determinant of M will be multiplied by λ. Thus if the determinant of $M = \begin{bmatrix} v_1 & v_2 \end{bmatrix}$ is $D \in \mathbb{F}_p^\times$, we choose instead $v_2' = D^{-1}v_2$ so that $M' = \begin{bmatrix} v_1 & v_2' \end{bmatrix} \in SL_2(\mathbb{F}_p)$. Thus we must divide by $|\mathbb{F}_p^\times| = (p-1)$ to get the desired cardinality.

5.1 We observe that any skew-symmetric matrix M has zeroes on the diagonal and satisfies $M_{ij} = -M_{ji}$ when $i \neq j$. We first show that

$$\text{Symm} \ + \ \text{Skew} = \text{All Matrices}$$

If M is a general matrix, then let $A = \frac{1}{2}(M + M^t)$ and $B = \frac{1}{2}(M - M^t)$. It is easy to see that $M = A + B$ and A is symmetric while B is skew-symmetric.

To show that this sum is direct, we must conclude that $\text{Symm} \cap \text{Skew} = \{\text{Zero Matrix}\}$. But if $A = A^t = -A$ then all entries $A_{ij} = -A_{ij}$, which means all entries of A are zero. This completes the proof.

5.2 There are multiple possible answers for W_2. The two easiest answers are the following:

Answer 1: W_2 is the set of matrices λI_n where $\lambda \in \mathbb{R}$ and I_n is the $n \times n$ identity matrix.

Let us show that $\mathbb{R}^{n\times n} = W_1 \oplus W_2$.

First, $W_1 + W_2 = \mathbb{R}^{n\times n}$, since if A is a general matrix, with trace λ, let $B = (A - (\lambda/n)I_n)$ and $C = (\lambda/n)I_n$. Clearly $A = B + C$, and $trB = trA - tr(\lambda/n)I_n = 0$ Thus $B \in W_1$ and $C \in W_2$.

Secondly, $W_1 \cap W_2 = \{zero\ matrix\}$ since the only multiple of the identity with trace zero is the zero matrix.

Answer 2: W_2 is the set of matrices λE_{nn} where $\lambda \in \mathbb{R}$ and E_{nn} has a 1 is the last row and last column and is zero elsewhere.

We can apply a similar approach, or try to construct explicit basis for $\mathbb{R}^{n\times n}$ that decomposes into W_1 and W_2 this way. In particular, one can show that $\mathbb{R}^{n\times n}$ has basis given by

$$\{E_{ij}\}_{i=1..n, j=1..n, i\neq j} \cup \{E_{11} - E_{22}, E_{22} - E_{33}, \ldots, E_{n-1,n-1} - E_{nn}\} \cup \{E_{nn}\}$$

Note that all but the last element give a basis for W_1 and E_{nn} spans W_2. We leave it to the reader to show that this is indeed a basis for $\mathbb{R}^{n\times n}$ but note that the number of elements is indeed $n(n-1)+(n-1)+1 = n^2$.

Problems from Chapter 4 of Artin's Algebra:

1.3 By the rank-nullity theorem, we know that

$$\dim Nullspace(A) + \dim Im(A) = n.$$

Further, $Im(A)$ is a subspace of $\mathbb{R}^m$ so $\dim Im(A) \leq m$. Thus the left-hand-side of the above equation is less than or equal to $\dim Nullspace(A) + m$. Subtracting m from both sides, we get

$$n \leq \dim Nullspace(A) + m, \quad \text{thus} \quad n - m \leq \dim Nullspace(A).$$

1.4 If a matrix M has rank 1, its nullsapce has dimension $n-1$ hence its row-reduced from would have a pivot in only one of the n columns. Consequently, we must have at least one nonzero column X, and all other columns are scalar multiples of the first one. Putting together these scalar multiple as a row-vector Y^t, we have $M = XY^t$ exactly as desired. Such vectors are not unique as we can divide all entries of X by λ by simultaneously multiplying all entries of Y^t by λ.

2.3 A point on the line $y = x$ looks like $\begin{bmatrix}\lambda\\ \lambda\end{bmatrix}$, and the image of $\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}\lambda\\ \lambda\end{bmatrix}$ is $\begin{bmatrix}\lambda(a+b)\\ \lambda(c+d)\end{bmatrix}$. Thus we want a, b, c, and d so that the point $\begin{bmatrix}\lambda(a+b)\\ \lambda(c+d)\end{bmatrix}$ is on the line $y = 3x$. Hence, we want $(c+d)$ to be $3(a+b)$. We also want $a + b \neq 0$ so that the linear operator does not simply send the line $y = x$ to the point $\begin{bmatrix}0\\ 0\end{bmatrix}$.

Thus, the set of such matrices are those of the form $\left\{\begin{bmatrix}a & b\\ c & 3a+3b-c\end{bmatrix} : a, b, c \in \mathbb{R}, a+b \neq 0\right\}$.

Not needed for the problem: Notice that the determinant of this matrix is $a(3a+3b-c) - bc = (3a-c)(a+b)$. We are assuming that $a + b \neq 0$ so that we do not collapse the line $y = x$ to the origin. If $3a - c = 0$ this linear operator still does the desired transformation but in fact will send all points in $\mathbb{R}^2$ to the line $y = 3x$. Finally, if neither of these quantities are zero then the linear operator is invertible sending $\mathbb{R}^2$ to $\mathbb{R}^2$ and happens to send the subspace given by the line $y = x$ to the subspace given by the line $y = 3x$.

Math 5285H: Fundamental Structures of Algebra I

HW 4 Solutions, (November 9th, 2011)

Problems from Chapter 4 of Artin's Algebra:

3.2 a) We must show that there exists $M \in GL_2(\mathbb{R})$ such that $M^{-1}\begin{bmatrix} a & b \\ c & d \end{bmatrix} M = \begin{bmatrix} 0 & b' \\ c' & d' \end{bmatrix}$ whenever $c \neq 0$. Letting $M = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$, we note that $M^{-1}\begin{bmatrix} a & b \\ c & d \end{bmatrix} M$ has top left entry $\frac{1}{eh-fg}(aeh - cef + bgh - dfg)$. So for example, let $M = \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} 1 & \frac{a}{c} \\ 0 & 1 \end{bmatrix}$ and the top left entry of the desired conjugate matrix becomes $a(1)(1) - c(1)(\frac{a}{c}) + b(0)(1) - d(\frac{a}{c})(0) = 0$. (Note that we use $c \neq 0$ since one of the entries of M used is a fraction with c in the denominator.)

Another way of seeing this is to say that $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is the matrix of some linear transformation $L : \mathbb{R}^2 \to \mathbb{R}^2$ using the standard basis $\{\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}\}$. By using the basis $\{\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} \frac{a}{c} \\ 1 \end{bmatrix}\}$ instead, we see that L would be written as $\begin{bmatrix} 0 & b - \frac{ad}{c} \\ c & a + d \end{bmatrix}$ in matrix form since

$$\begin{aligned} \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} &= 0 \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} + c \cdot \begin{bmatrix} \frac{a}{c} \\ 1 \end{bmatrix}, \text{ and} \\ \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} \frac{a}{c} \\ 1 \end{bmatrix} &= \left(b - \frac{ad}{c}\right) \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} + (a+d) \cdot \begin{bmatrix} \frac{a}{c} \\ 1 \end{bmatrix}. \end{aligned}$$

There are also other change of bases (i.e. matrices M) that result in the desired zero in the top left entry.

b) We claim that $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ is similar to a matrix of the form $\begin{bmatrix} 0 & b' \\ c' & d' \end{bmatrix}$ unless $a = d$ and $b = 0$. Thus we need to show that there exists $M = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$ such that $M^{-1}\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} M = \begin{bmatrix} 0 & b' \\ c' & d' \end{bmatrix}$ (except in the case mentioned). Or equivalently show that there is a basis $\{M_1, M_2\}$ such that $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} M_1 = c'M_2$ and $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} M_2 = b'M_1 + d'M_2$.

Case 1: $a \neq d$ and $b = 0$. Let $M = \begin{bmatrix} d & a \\ 1 & 1 \end{bmatrix}$. Then $\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} M_1 = dM_2$ and $\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} M_2 = -aM_1 + (a+d)M_2$. Since $a \neq d$, M is in fact invertible (i.e. $\{M_1, M_2\}$ is a basis) and we obtain $M^{-1} \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} M = \begin{bmatrix} 0 & -a \\ d & a+d \end{bmatrix}$.

Case 2: $b \neq 0$. Let $M = \begin{bmatrix} 1 & 0 \\ -\frac{a}{b} & -\frac{a}{b} \end{bmatrix}$ and we get that M is invertible and $M^{-1} \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} M = \begin{bmatrix} 0 & -a \\ d & a+d \end{bmatrix}$.

Remark: There are other explicit ways to illustrate the desired similarity of matrices in these cases. Alternatively, one could also note that when $a \neq d$, then the matrix $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ has two distinct eigenvalues ($a \neq d$) and so is diagonalizable. If the case $a = d$ and $b \neq 0$, then the Jordan form of $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$ is $\begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}$. Analogously matrix $\begin{bmatrix} 0 & -a \\ d & a+d \end{bmatrix}$ is diagonalizable if $a \neq d$, and when $a = d$ and $b \neq 0$, the eigenspace corresponding to eigenvalue a is only one-dimensional and the Jordan form is $\begin{bmatrix} a & 1 \\ 0 & a \end{bmatrix}$. Thus by transitivity and symmetry of similarity as an equivalence relation, we get that $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ is similar to $\begin{bmatrix} 0 & -a \\ d & a+d \end{bmatrix}$.

(Note also that we guess a similar matrix of this form since similar matrices have the same eigenvalues and so the same trace and determinant as each other.)

Case 3: We now consider the case $a = d$ and $b = 0$. We wish to show such a matrix is **not** similar to one of the form $\begin{bmatrix} 0 & b' \\ c' & d' \end{bmatrix}$ in this case. Clearly the matrices M used in the above two cases are rank 1, i.e. not invertible, under these assumptions. However, this is not enough to say that there is not another type of matrix M that does work.

Since similar matrices have the same eigenvalues, the matrix $\begin{bmatrix} 0 & b' \\ c' & d' \end{bmatrix}$ must be of the form $\begin{bmatrix} 0 & -aC \\ d/C & a+d \end{bmatrix}$ for some nonzero C. It thus suffices to show that the matrix $A = \begin{bmatrix} 0 & -aC \\ a/C & 2a \end{bmatrix}$ is not diagonalizable. Note first that $v = \begin{bmatrix} -C \\ 1 \end{bmatrix}$ is an eigenvector for this matrix (with eigenvalue a). Further by looking at the characteristic equation and nullspace of $A - aI = \begin{bmatrix} -a & -aC \\ a/C & a \end{bmatrix}$, we see that there are no other eigenvectors that would be linearly independent with v. Thus A is not diagonalizable and cannot be similar to $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$.

4.1 Firstly, the eigenspace $V^{(\lambda)}$ is a *subspace* since if v_1 and v_2 are in $V^{(\lambda)}$ and c_1, c_2 are scalars, then the vector $T(c_1v_1 + c_2v_2) = c_1T(v_1) + c_2T(V_2) = c_1(\lambda v_1) + c_2(\lambda v_2) = \lambda(c_1v_1 + c_2v_2)$. Thus $c_1v_1 + c_2v_2 \in V^{(\lambda)}$ as well. We now show that $V^{(\lambda)}$ is T-*invariant*. This follows since $T(v) = \lambda v$ if $v \in V^{(\lambda)}$ and $\lambda v \in V^{(\lambda)}$ since we showed $V^{(\lambda)}$ is a subspace, hence closed under scalar multiplication.

4.2 a) Assuming that T^2 is the identity operator on vector space V, we have that $I - T^2 = (I + T)(I - T)$ is the zero map that sends all vectors in V to zero.

Remark: In general, one must be careful when factoring polynomials involving linear operators. However, since $IT = TI = T$, this factorization actually works. Note also that this factorization signifies an **ordered** composition of linear operators.

Proceeding, for $v \in V$, we thus have that $(I + T)(I - T)v = \mathbf{0}$. In other words, $(I + T)(v - Tv) = \mathbf{0}$. Letting $w = v - Tv$, we thus conclude that $w + Tw = \mathbf{0}$, i.e. $Tw = -w$. Hence, either $w = 0$ or w is an eigenvector with eiegnvalue -1.

To see that $V = V^{(1)} \oplus V^{(-1)}$, we first note that $V^{(1)} \cap V^{(-1)} = \{\mathbf{0}\}$ since if w is a (non-zero) eigenvector with eigenvalue 1 and eigenvalue -1, we would get $Tw = w = -w$, which is a contradiction. Thus, it suffices to show that $V = V^{(1)} + V^{(-1)}$ when V has the property that $T^2 = I$ on V.

For any v in V, we can write $v = \frac{v-Tv}{2} + \frac{v+Tv}{2}$. Since scalar multiplication does not change whether a vector is an eigenvector, we have that $\frac{v-Tv}{2} \in V^{(-1)}$. By analogous logic, i.e. factoring $I - T^2 = (I - T)(I + T)$ instead, we get that $\frac{v+Tv}{2} \in V^{(1)}$, completing the proof.

Answer 2: Also notice that we can show $V = V^{(1)} + V^{(-1)}$ without factoring the polynomial $(I - T^2)$. Again write $v = \frac{v-Tv}{2} + \frac{v+Tv}{2}$. Then we use the facts that

$$\begin{aligned} T\left(\frac{v - Tv}{2}\right) &= \frac{Tv - T^2v}{2} = \frac{Tv - v}{2} = -\left(\frac{v - Tv}{2}\right) \quad \text{and} \\ T\left(\frac{v + Tv}{2}\right) &= \frac{Tv + T^2v}{2} = \frac{Tv + v}{2} = +\left(\frac{v + Tv}{2}\right) \end{aligned}$$

to conclude that v is the sum of an eigenvector with eigenvalue -1 and an eigenvector with eigenvalue $+1$.

b) If V is a complex vector space, we can write

$$v = \frac{v + Tv + T^2v + T^3v}{4} + \frac{v - Tv + T^2v - T^3v}{4} + \frac{v - iTv - T^2v + iT^3v}{4} + \frac{v + iTv - T^2v - iT^3v}{4}$$

where $i = \sqrt{-1}$. We claim that $V = V^{(-1)} \oplus V^{(-i)} \oplus V^{(1)} \oplus V^{(i)}$. It is clear that each pairwise intersection is $\{\mathbf{0}\}$, so it suffices to show that $v_1 = \frac{v+Tv+T^2v+T^3v}{4} \in V^{(1)}$, $v_{-1} = \frac{v-Tv+T^2v-T^3v}{4} \in V^{(-1)}$, $v_{-i} = \frac{v-iTv-T^2v+iT^3v}{4} \in V^{(-i)}$, and $v_i = \frac{v+iTv-T^2v-iT^3v}{4} \in V^{(i)}$.

We use the facts that $T^4v = v$ and that T is linear, and deduce that $Tv_\alpha = \alpha \cdot v_\alpha$ for $\alpha \in \{1, i, -1, -i\}$.

6.8 If T is nilpotent, i.e. $T^k = 0$ for some k, and if v was an eigenvector with eigenvalue λ, then $Tv = \lambda v$ and $T^kv = \lambda^k v$. But $T^kv = 0$, so we get $\lambda = 0$. Thus, for any nilpotent operator, all eigenvalues of T are zero.

We then use Corollary 4.6.3, which states that for any linear operator T with all eigenvalues in a field F, there exists a basis such that T can be expressed as an upper-triangular matrix (with entries in F). *Note*

that we didn't prove this in class, but since this is linear algebra, I will not require you to reprove it for the homework. As in the book, this can be proven by induction picking one eigenvector (with eigenvalue in F) at a time. Thus the diagonal entries should be the eigenvalues of T, which are all zero, hence we have the desired form.

We now need to prove the other direction. If there is a basis so that the matrix corresponding to T is upper triangular with zeros on the diagonal, then the matrix corresponding to T^2 would be upper-triangular with zeros on both the diagonal and super-diagonal. Continuing in this way, if the matrix was n-by-n, then T^n would be the zero matrix with respect to this basis. This such a T is nilpotent.

Problems from Chapter 5 of Artin's Algebra:

1.1 **We write all of these matrices are with respect to the standard bases.** We compute these matrices by writing them down with respect to a orthonormal basis and then by conjugating by the inverse of the basechange matrix. We write down the orthonormal bases in such an order so that the first column is the unit vector fixed by the rotation (the pole) and the second and third are ordered so that the determinant of $B = [B_1, B_2, B_3]$ is 1 (as opposed to -1). In particular, we are using (b) of Corollary 5.1.28 where we let $u = \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \right\}$, and $u' = Bu$ is the desired pole. The choice of orthonormal basis for the two-dimensional subspace $Span(u)^{\perp}$ is irrelevant as long as the order is chosen so that matrix B has positive determinant.

Remark: If you wrote down a matrix with respect to *a different basis* (i.e. other than the standard one) you will get credit if your basis is *clearly* written down.

(a) We use the orthonormal basis $\{e_2, e_3, e_1\}$. With respect to this basis, the associated linear transformation has matrix $M = \begin{bmatrix} 1 & 0 & 0 \\ 0 & cos\theta & -sin\theta \\ 0 & sin\theta & cos\theta \end{bmatrix}$. Conjugating by B^{-1} where $B = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$, we obtain $BMB^{-1} = \begin{bmatrix} cos\theta & 0 & sin\theta \\ 0 & 1 & 0 \\ -sin\theta & 0 & cos\theta \end{bmatrix}$.

(b) We use the orthonormal basis $\left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \Big/ \sqrt{3}, \quad \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix} \Big/ \sqrt{2}, \quad \begin{bmatrix} 1/2 \\ 1/2 \\ -1 \end{bmatrix} \Big/ \sqrt{\tfrac{3}{2}} \right\}$. With respect to this basis, the associated linear transformation looks like $\begin{bmatrix} 1 & 0 & 0 \\ 0 & -\frac{\sqrt{3}}{2} & 1/2 \\ 0 & -1/2 & -\frac{\sqrt{3}}{2} \end{bmatrix}$. Conjugating by B^{-1}, where B's columns are the basis elements, we get $\begin{bmatrix} 1/3 - \sqrt{3}/3 & 1/3 + \sqrt{3}/3 & 1/3 \\ 1/3 & 1/3 - \sqrt{3}/3 & 1/3 + \sqrt{3}/3 \\ 1/3 + \sqrt{3}/3 & 1/3 & 1/3 - \sqrt{3}/3 \end{bmatrix}$.

(c) We use the orthonormal basis $\left\{ \begin{bmatrix}1\\1\\0\end{bmatrix} \Big/ \sqrt{2}, \quad \begin{bmatrix}0\\0\\1\end{bmatrix}, \quad \begin{bmatrix}1\\-1\\0\end{bmatrix} \Big/ \sqrt{2} \right\}$. With respect to this basis, the associated linear transformation looks like $\begin{bmatrix}1 & 0 & 0\\0 & 0 & 1\\0 & -1 & 0\end{bmatrix}$. Conjugating by B^{-1}, where B's columns are the basis elements, we get $\begin{bmatrix}1/2 & 1/2 & -\sqrt{2}/2\\1/2 & 1/2 & \sqrt{2}/2\\\sqrt{2}/2 & -\sqrt{2}/2 & 0\end{bmatrix}$.

1.3 Recall from Proposition 2.11.4 that if H and K are subgroups of G then $H \times K \cong G$ by the multiplication map if and only if $H \cap K = \{1\}$, $HK = G$ and both H and K are normal subgroups of G.

In this case, $G = O_n$, $H = SO_n$ and $K = \{\pm I_n\}$. Notice that $det(-I_n) = (-1)^n$ so $H \cap K = \{I_n\}$ if n is odd but $H \cap K = \{-I_n, I_n\}$ if n is even.

In the case that n is odd however, $-I_n$ corresponds to a reflection and any matrix $M \in O_n$ with determinant -1 (i.e. a reflection) satsfies $\det(M(-I_n)) = +1$ and is in SO_n. Thus, $HK = G$ in this case, as we can write any M in SO_n as $M \cdot I_n$ and any $M \in O_n \setminus SO_n$ as $(-M) \cdot (-I_n)$. We lastly have to verify that H and K are both normal subgroups when n is odd. Clearly, $(\pm h)H(\pm h^{-1}) = H$ for $h \in H$ hence H is a normal subgroup of G. Furthermore, $(\pm h)(-I_n)(\pm h^{-1}) = -I_n$, so K is a normal subgroup too.

Thus $O_n \cong SO_n \times \{\pm I_n\}$ if and only if n is odd.

M.1 (for $n = 2$ and 3)

In the case $n = 2$, any matrix in $O_2(\mathbb{R})$ looks like $\begin{bmatrix}cos\theta & \mp sin\theta\\sin\theta & \pm cos\theta\end{bmatrix}$. Such a matrix is in $O_2(\mathbb{Z})$ only if $cos\theta$ and $sin\theta$ are both integers (i.e. $\theta = 0, \pi/2, \pi$, or $3\pi/2$). Thus

$$O_2(\mathbb{Z}) = \left\{ \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}, \begin{bmatrix}-1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}-1 & 0\\0 & -1\end{bmatrix}, \begin{bmatrix}0 & 1\\-1 & 0\end{bmatrix}, \begin{bmatrix}0 & -1\\1 & 0\end{bmatrix}, \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}, \begin{bmatrix}0 & -1\\-1 & 0\end{bmatrix} \right\} \cong D_4.$$

For general n, we note that each column of $M \in O_n(\mathbb{Z})$ is a vector of length one (since the columns of an orthogonal matrix are an orthonormal basis). The only unit vectors with integer entries are $\pm e_i$. Thus $O_n(\mathbb{Z})$ is the set of signed permutation matrices, which contain exactly one nonzero entry in each row and column and have ± 1 as their nonzero entries.

Another interpretation of $O_n(\mathbb{Z})$ is as the symmetries of the signed unit vectors $\{\pm e_1, \pm e_2, \ldots, \pm e_n\}$. Looking at the dual of these vectors, we get that $O_n(\mathbb{Z})$ is the group of symmetries of the hypercube.

In particular $O_3(\mathbb{Z})$ is the group of symmetries of the (usual 3-dimensional) cube. We will see this group again in a week or two. Its order is size $48 = 2^3 \cdot 3!$.

M.5 a) **NOTE:** There is a typo in this problem (in some printings of the book). It should say:

Prove the formula

$$f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

While this problem can be solved combinatorially or induction, here we give a proof via techniques from linear algebra.

The eigenvalues of $M = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ are roots of the characteristic polynomial $x^2 - (trace)x + (det) = x^2 - x - 1$.

The roots are thus $\lambda_{1,2} = \frac{1\pm\sqrt{5}}{2}$. Consequently, there exists invertible P such that $P^{-1}MP = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$.

In particular, $P = [P_1 P_2]$ where P_i is the eigenvector of M with eigenvalue λ_i, written as a column vector. In this case, $P = \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix}$ and $P^{-1} = \begin{bmatrix} 1/2 - \sqrt{5}/10 & 1/\sqrt{5} \\ 1/2 + \sqrt{5}/10 & -1/\sqrt{5} \end{bmatrix}$.

Since the Fibonacci numbers satisfy $M \begin{bmatrix} f_{n-2} \\ f_{n-1} \end{bmatrix} = \begin{bmatrix} f_{n-1} \\ f_n \end{bmatrix}$, it follows that $M^n \begin{bmatrix} 0 \\ 1 \end{bmatrix} = M^n \begin{bmatrix} f_0 \\ f_1 \end{bmatrix} = \begin{bmatrix} f_n \\ f_{n+1} \end{bmatrix}$.

And so, $(P^{-1}MP)^n = P^{-1}M^nP$ applied to $P^{-1}\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ will equal $P^{-1}M^n(PP^{-1})\begin{bmatrix} f_0 \\ f_1 \end{bmatrix} = P^{-1}\begin{bmatrix} f_n \\ f_{n+1} \end{bmatrix}$. Thus $P^{-1}\begin{bmatrix} f_n \\ f_{n+1} \end{bmatrix} = \begin{bmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{bmatrix} P^{-1}\begin{bmatrix} 0 \\ 1 \end{bmatrix}$, which implies that

$$\begin{bmatrix} f_n \\ f_{n+1} \end{bmatrix} = P\begin{bmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{bmatrix} P^{-1}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = P\begin{bmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{bmatrix}\begin{bmatrix} 1/\sqrt{5} \\ -1/\sqrt{5} \end{bmatrix} = P\begin{bmatrix} \lambda_1^n/\sqrt{5} \\ -\lambda_2^n/\sqrt{5} \end{bmatrix}.$$

Plugging in P from above and looking at the top row, we conclude $f_n = \frac{1}{\sqrt{5}}\lambda_1^n - \frac{1}{\sqrt{5}}\lambda_2^n$ as desired.

b) By similar logic, we find that $a_n = c_1\lambda_1^n + c_2\lambda_2^n$ where c_1 and c_2 are some constants and $\lambda_{1,2}$ are the eigenvalues of the matrix $\begin{bmatrix} 0 & 1 \\ 1/2 & 1/2 \end{bmatrix}$. Since the characteristic polynomial is $x^2 - \frac{x}{2} - \frac{1}{2} = (x-1)(x+1/2)$, λ_1 and λ_2 are 1 and $-1/2$. Letting $n = 0$ and $n = 1$ we get that $c_1 + c_2 = a_0$ and $c_1(1) + c_2(-1/2) = a_1$. Solving this linear system, we obtain

$$c_1 = \frac{a_0}{3} + \frac{2a_1}{3} \quad \text{and} \quad c_2 = \frac{2a_0}{3} - \frac{2a_1}{3}.$$

Thus $\lim_{n\to\infty} a_n = c_1(1)^n + c_2(-1/2)^n = \frac{a_0}{3} + \frac{2a_1}{3}$.

Problems from Chapter 6 of Artin's Algebra:

3.2 If m is an orientation-reversing isometry, then m has the algebraic form $m = t_{\mathbf{a}}\rho_\theta r$ where $\mathbf{a}$ or θ could be zero and r is reflection about the x-axis. Then

$$\begin{aligned} m^2 &= (t_{\mathbf{a}}\ \rho_\theta\ r)\ t_{\mathbf{a}}\ (\rho_\theta\ r) = t_{\mathbf{a}}\ \rho_\theta\ r\ (t_{\mathbf{a}}\ r)\ \rho_{-\theta} = t_{\mathbf{a}}\ \rho_\theta\ r^2\ t_{\mathbf{a}'}\ \rho_{-\theta} \\ &= t_{\mathbf{a}}\ (\rho_\theta\ t_{\mathbf{a}'})\ \rho_{-\theta} = t_{\mathbf{a}}\ t_{\mathbf{a}''}\ \rho_\theta\ \rho_{-\theta} = t_{\mathbf{a}+\mathbf{a}''}\ \rho_{\theta+(-\theta)} = t_{\mathbf{a}+\mathbf{a}''}. \end{aligned}$$

Here, $\mathbf{a}' = r(\mathbf{a})$ and $\mathbf{a}'' = \rho_\theta(\mathbf{a}')$.

3.3 If linear operator ϕ is a reflection, $\phi = \rho_\theta r$ for some angle θ. In other words, ϕ is a reflection about the line ℓ through the origin which makes an angle of $\theta/2$ with the x-axis. Thus the matrix for such a ϕ is $M = \begin{bmatrix} cos\theta & sin\theta \\ sin\theta & -cos\theta \end{bmatrix}$. If $\theta = 0$ or π, then $M = \begin{bmatrix} \pm 1 & 0 \\ 0 & \mp 1 \end{bmatrix}$ and the orthogonal eigenvector with the desired eigenvalues are the standard basis vectors. As long as $\theta \neq 0, \pi$, let $v_1 = \begin{bmatrix} cos\theta + 1 \\ sin\theta \end{bmatrix}$ and $v_2 = \begin{bmatrix} cos\theta - 1 \\ sin\theta \end{bmatrix}$. We see that $Mv_1 = v_1$, $Mv_2 = -v_2$, and the dot product $v_1 \cdot v_2 = 0$. Thus a reflection has the desired orthogonal eigenvectors.

Proving the other direction, let M be a matrix with two orthogonal eigenvectors (of length one) P_1 and P_2 with eigenvalues 1 and -1, respectively. Let $P = [P_1 P_2]$ and $PMP^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ and since P's columns are an orthonormal basis, the matrix P is orthogonal. Picking the order of the basis so that $\det P = +1$, matrix $P \in SO_2(\mathbb{R})$, thus is a rotation. The conjugate of a reflection by a rotation is again a reflection ($\rho_\theta r \rho_{-\theta} = \rho_{2\theta} r$), thus we have the desired result.

3.4 Conjugating by an isometry ϕ corresponds to applying a coordinate change. This conjugation sends the glide-reflection to a glide-reflection where the axis of reflection is rotated and translated to another line. If it is orientation-reversing, the glide vector might be reflected as well. However, since multiplication by an isometry preserves lengths, the length of the glide vector is preserved.

4.1 In D_n, we have $x^n = 1$, $y^2 = 1$, and $yx = x^{-1}y$. Thus

$$x^2yx^{-1}y^{-1}x^3y^3 = x^2yx^{-1}(yx^3)y = x^2yx^{-1}x^{-3}y^2 = x^2(yx^{-4}) = x^2x^4y = x^6y.$$

4.2 a) Since a subgroup of $D_4 = \langle x, y \rangle$ is a finite subgroup of isometries, we know that any such subgroup either is cyclic (generated by a rotation) or isomorphic to a smaller dihedral group.

Cyclic subgroups: $\{1\}, \{1, x^2\}, \{1, x, x^2, x^3\}$. Notice that each of the eight elements generates a cyclic subgroup except that both x and x^3 generate the same cyclic subgroup.

Dihedral subgroups: $\{1, y\}, \{1, xy\}, \{1, x^2y\}, \{1, x^3y\}, \{1, x^2, y, x^2y\}$, $\{1, x^2, xy, x^3y\}$, and D_4 itself. Note that a dihedral subgroup of D_n is generated by a reflection and a rotation of order $m \geq 1$ where $m|n$.

To determine which of these are normal, we note that $x^{-i}x^jx^i = x^j$ and $x^{-i}(x^jy)x^i = x^{j-2i}y$.

We also have $(x^iy)^{-1}(x^j)(x^iy) = yx^{-i}x^jx^iy = yx^jy = x^{-j}$, which is the inverse of x^j, and $(x^iy)^{-1}(x^jy)(x^iy) = yx^{-i}x^jyx^iy = yx^{-i}x^jx^{-i}y^2 = x^{j-2i}y$.

Consequently, a subgroup H of D_n is normal if and only if it contains $x^{j-2i}y$ for all $i \in \{0, 1, 2, \ldots, n-1\}$ whenever H contains x^jy. For $n = 4$, that means that H contains $x^{j+2}y$ if H contains x^jy.

Thus the normal subgroups of D_4 are the cyclic subgroups containing only powers of x, and the dihedral subgroups containing either both y and x^2y or both xy and x^3y:

$$\{1\}, \{1, x^2\}, \{1, x, x^2, x^3\}, \{1, x^2, y, x^2y\}, \{1, x^2, xy, x^3y\}, \text{ and } D_4.$$

b) Using analogous logic, the proper normal subgroups of D_{15} are those cyclic subgroups, generated by a rotation, or a dihedral subgroup H which contains $x^{j-2}y, x^{j-4}y, \ldots, x^{j-28}y$ whenever H contains x^jy. However, $gcd(2, 15) = 1$, so (unlike the last example) we find that $\{x^{j-2}y, \ldots, x^{j-13}y\} = \{y, xy, x^2y, \ldots, x^{14}y\}$. In other words, a dihedral subgroup H of D_{15} can only be normal if it contains all 15 reflections once it contains a single reflection. Further, if H contains y and x^iy, H also contains the rotation x^i.

In conclusion, the only proper normal subgroups of D_{15} are $C_3 = \{1, x^5, x^{10}\}$, $C_5 = \{1, x^3, x^6, x^9, x^{12}\}$, and $C_{15} = \{1, x, x^2, \ldots, x^{14}\}$. The quotient group $D_{15}/C_3 \cong \{1, x, x^2, x^3, x^4, y, xy, x^2y, x^3y, x^4y\} = D_5$, the quotient group $D_{15}/C_5 \cong \{1, x, x^2, y, xyx^2y\} = D_3$, and $D_{15}/C_{15} \cong \{1, y\} = D_1$.

Note: To see these isomorphisms, we use the maps π_5, π_3, and π_1 such that $\pi_k(x^j) \mapsto x^{j \mod k}$

(in particular, $\pi_i(x^i) \mapsto 1$), $\pi_i(y) \mapsto y$, and we extend linearly. The image of each of these maps are D_5, D_3, and D_1, respectively with kernels C_3, C_5, and C_{15}. Thus we get the isomorphism types of these quotient groups by the First Isomorphism Theorem.

c) $\{1\}$, $\{1, x^2, x^4\}$, $\{1, y\}$, $\{1, xy\}$, $\{1, x^2y\}$, $\{1, x^3y\}$, $\{1, x^4y\}$, $\{1, x^5y\}$,
$\{1, x^2, x^4, y, x^2y, x^4y\}$, $\{1, x^2, x^4, xy, x^3y, x^5y\}$.

4.3 a) Since $x^{-5} = x^5$, i.e. $yx^5 = x^5y$, in D_{10}, the left cosets of $H = \{1, x^5\}$ in D_{10} are

$$\{1, x^5\}, \{x, x^6\}, \{x^2, x^7\}, \{x^3, x^8\}, \{x^4, x^9\}, \{y, x^5y\}, \{xy, x^6y\}, \{x^2y, x^7y\}, \{x^3y, x^8y\}, \{x^4y, x^9y\}.$$

b) It follows that the right cosets of $\{1, x^5\}$ are the same partition of D_{10}, thus $\{1, x^5\}$ is a normal subgroup.

Notice that $(x^5g)h = x^5gh$, $g(x^5h) = x^5gh$, and $(x^5g)(x^5h) = gh$ so letting $\overline{g}$ represent the left-coset $\{g, x^5g\}$ it follows that the quotient group $D_{10}/H \cong D_5$ by using the map $\pi : D_{10} \to D_5$, via $\pi(x^5) = 1$ and $\pi(y) = y$, which has kernel H.

c) Yes, $D_{10} \cong D_5 \times \{1, x^5\} = K \times H$. To see this, note that K and H are both normal subgroups of D_{10} (we already showed that H is normal and K is normal because it is of index 2, hence the only conjugate subgroup of that size), $D_{10} = HK$ and $H \cap K = \{1\}$.

5.1 By a coordinate change, i.e. conjugating all elements of the group $G = \langle r_1, r_2 \rangle$ by a certain rotation, we can assume that $r_1 = r$, reflection about the x-axis. Under these coordinates, $r_2 = \rho_{2\theta}r = \rho_\theta r \rho_{-\theta}$ where $\theta = \pi/n$. Thus (r_2r_1) is the rotation $\rho_{2\pi/n}$ which is of order n. Instead of thinking of G being generated by r_1 and r_2, we can equivalently consider it to be generated by r_1 and rotation $\rho_{2\pi/n} = r_2r_1$ (since $r_2 = (r_2r_1)r_1$). Thus we see G is generated by a rotation of order n and a reflection about a line through the origin, and hence is a dihedral group D_n.

Math 5285H: Fundamental Structures of Algebra I

HW 5 Solutions, (December 7th, 2011)

Problems from Chapter 6 of Artin's Algebra.

7.1 Label the four vertices of the square in clockwise order as A, B, C, D. Then let the Dihedral group $D_4 = \{1, \rho, \rho^2, \rho^3, r, \rho r, \rho^2 r, \rho^3 r\}$ where $\rho = (ABCD)$ is clockwise rotation by $\pi/2$ and $r = (AD)(BC)$ is reflection about the horizontal axis.

a) The stabilizer of the vertex A is the subgroup $\{1, \rho r\}$.

Notice that $\rho r = (ABCD)(AD)(BC) = (A)(BD)(C)$, reflection about the BD diagonal-axis, so 1 and ρr are both in the stabilizer subgroup. Further, D_4 acts transitively on the vertices, hence the order of the stabilizer is $|D_4|/|O_A| = 8/4 = 2$, and we have thus found the entire stabilizer subgroup.

Note: the stabilizer of any vertex v is also an order 2 subgroup generated by reflection about the diagonal axis incident to v.

The stabilizer of the edge AD is the subgroup $\{1, r\}$. Again, D_4 acts transitively on the four edges and so we again get the stabilizer has order 2.

b) Consider the diagonal AC (without loss of generality). D_4 acts transitively on the set of diagonals, $\{AC, BD\}$, and so the stabilizer subgroup has order $|D_4|/|O_{AC}| = 8/2 = 4$.

By inspection, the stabilizer of AC is $\{1, \rho^2, \rho r, \rho^3 r\}$ since $\rho^2 = (ABCD)(ABCD) = (AC)(BD)$, $\rho r = (A)(BD)(C)$, and $\rho^3 r = (DCBA)(AD)(BC) = (AC)(B)(D)$.

7.3 a) First we conisder how S_3 can act transitively on a set U of cardinality three.

Lemma: Up to relabelling, a *transitive* action of S_3 on $U = \{u_1, u_2, u_3\}$ must act in the natural way, i.e. for $\sigma \in S_3$, we have $\sigma(u_i) = u_{\sigma(i)}$.

Proof: Consider $u_1 \in U$. The size of the stabilizer G_{u_1} is $|S_3|/|O_{u_1}| = 2$ so there exists $g \in S_3$ such that $g \neq 1$ and $g(u_1) = u_1$. Since g induces a bijection, either g acts trivially or $g(u_2) = u_3$ and $g(u_3) = u_2$. However, an action of S_3 on U induces a permutation representation, i.e. a homomorphism $\phi : S_3 \to Perm(U) \cong S_3$. Hence g cannot act trivially, because otherwise Ker $\phi = \{1, g\}$ which would be a normal subgroup of S_3. But S_3 contains no normal subgroups of size 2, hence g acts on U by

sending $(u_1, u_2, u_3) \to (u_1, u_3, u_2)$. Similarly, by considering G_{u_2} and G_{u_3}, we see that S_3 contains elements g, g', g'', all pairwise distinct, that fix one element and transpose the other two. Thus Im ϕ contains all three transpositions, which generate S_3. Hence, up to relabeling (i.e. an automorphism of S_3), a transitive action of S_3 on $U = \{u_1, u_2, u_3\}$ must act in the natural way.

Assume that U and V are both labeled so that S_3 acts naturally on both sets. Then we obtain two orbits:

$$\{(u_1, v_1), (u_2, v_2), (u_3, v_3)\} \quad \text{and} \quad \{(u_1, v_2), (u_1, v_3), (u_2, v_1), (u_2, v_3), (u_3, v_1), (u_3, v_2)\}.$$

This is seen by noting that $(u_i, v_i) \to (u_{\sigma(i)}, v_{\sigma(i)})$, which leads to the first orbit, and we apply permutations id, (23), (12), (123), (132), (13) to (u_1, v_2), respectively, for the second orbit.

b) Using the above lemma, we see that we can again label $U = \{u_1, u_2, u_3\}$ so that S_3 acts on U naturally (since S_3 acts on U transitively). With the supposed orbit structure, the permutation representation $\psi : S_3 \to Perm(V)$ is the map $\psi : S_3 \to \{1, (23)\}$, which has kernel $A_3 = \{1, (123), (132)\}$, a normal subgroup of S_3. By conjugating by an element in A_3, we see that all three transpositions in S_3 are conjugate to one another. It follows that S_3's action on V is defined as follows: $\sigma(v_1) = v_1$, $\sigma(v_2) = v_3$, $\sigma(v_3) = v_2$ if σ is a transposition, and σ acts trivially on V otherwise. Thus we again get two orbits:

$$\{(u_1, v_1), (u_2, v_1), (u_3, v_1)\}, \quad \text{and} \quad \{(u_1, v_2), (u_1, v_3), (u_2, v_2), (u_2, v_3), (u_3, v_2), (u_3, v_3)\}.$$

Here we see that for any $\sigma \in S_3$ $\sigma(v_1) = v_1$, which explains the first orbit. To see the second orbit, we act on (u_1, v_2) respectively by permutations id, (23), (123), (12), (132), and (13).

8.2 Let G act on the left-cosets G/H by left-multiplication. The stabilizer of the coset $[aH]$ is the set $\{g \in G : g[aH] = [aH]\} = \{g \in G : gah = ah' \text{ for } h, h' \in H\} = \{g \in aHa^{-1}\}$. Here the last equality of sets is obtained by multiplying on the right by $h^{-1}a^{-1}$.

10.2 Suppose G acts transitively on S and U is a subset of S. Then G also acts on S', the set of subsets V of S with cardinality $|V| = |U|$. Let $O_U = \{U, g_2U, \ldots, g_kU\}$ be the orbit of U under the action of G on S'. By construction G also acts transitively on O_U. Hence $O_U = O_{gU}$ for any $g \in G$, and hence for any $gU \in O_U$, we obtain $|\{h \in G : h(gU) = gU\}| = |G|/|O_U|$. Let H_{gU} denote this stabilizer. We also know that each of the stabilizers of a given element under the action of G on S all have the same cardinalities. Let us denote these as G_s for $s \in S$.

Then the desired result is to let $T_s = \{gU \in O_U : s \in gU\}$, and show that $|T_s| = |T_{s'}|$ for all $s, s' \in S$. By putting the above together, we see that for any $s \in gU \subset S$, we have $|T_s| = |H_{gU}|/|G_s|$ which is indepedent of the choice of s or gU.

11.1 If $G = S_3$ acts on a set S with $|S| = 4$, then this action induces a permutation representation $\phi : S_3 = G \to Perm(S) \cong S_4$ which is a homomorphism. As in problem (7.3), the kernel of ϕ must be a normal subgroup of S_3. However, the only normal subgroups of S_3 are $\{1\}$, A_3, and S_3.

If Ker $\phi = \{1\}$, then the group action is faithful and Im $\phi \cong S_3$ so that means that one of the four elements of S is fixed, and the other three are permuted naturally (and transitively).

If Ker $\phi = A_3$, then there are two cases:

Subcase 1: two of the four elements of S are fixed, and the other two are swapped by the action of any transposition. Any other permutation in S_3 acts trivially.

Subcase 2: we split the four elements of S into two subsets of two each. (e.g. $S = \{1, 2\} \cup \{3, 4\}$) Then any transposition acts by swapping both pairs, e.g. acts as $(12)(34)$. Any other permutation in S_3 acts trivially.

If Ker $\phi = S_3$, then S_3 simply acts on S trivially so that $\sigma(s_i) = s_i$ for all $\sigma \in S_3$ and all four $s_i \in S$.

Note that if the four elements of S are distinguishable from the start, there are $4 \cdot |Aut\ S_3| = 24$ ways for S_3 to act faithfully, $\binom{4}{2} = 6$ ways for S_3 to act such that Ker $\phi = A_3$ (for each subcase), and one way to act trivially.

Answer 2: If S_3 acts on S, a set of four elements, we note that each orbit O_i under this action must have $|O_i|$ divides $|S_3| = 6$. Since $|S| = 4$, the possible orbit decompositions are $|S| = 1 + 3$, $|S| = 1 + 1 + 2$, $|S| = 2 + 2$, or $|S| = 1 + 1 + 1 + 1$. We have seen these four actions exhibited above but must look at the kernel of the permutation representation or otherwise, to figure out the explicit action.

12.4 Let $S = \{T_1, T_2\}$ be the set of the two inscribed tetrahedra in the cube. To see these tetrahedra, pick one vertex v_1 of the cube and then let $\{v_2, v_3, v_4\}$ be the three vertices you can reach from v_1 by traversing exactly two edges. Let $\{v_1, v_2, v_3, v_4\}$ be the four vertices of tetrahedron T_1. To obtain T_2, use as corners the antipodal points, i.e. the other four vertices. The octahedral group O clearly acts on S and this action is transitive since rotation about a face by $\pi/4$ swaps the two tetrahedra. Thus $H = G_{T_1} = G_{T_2}$, the stabilizer of cardinality $|O|/|S| = 12$.

We show explicitly that for every specific rotation in tetrahedral group T, there is a corresponding rotation of the cube in H. Since $|H| = |T|$, this direction is sufficient. Note if we label the tetrahedron's vertices as A, B, C, and D, then T is generated by the 3-cycles $(ABC)(D)$, $(ABD)(C)$, $(ACD)(B)$ and $(BCD)(A)$. To see this, note that each of them can be squared to obtain eight 3-cycles, and then $(ABC)(D) \cdot (ABD)(C) = (AC)(BD)$ and we can obtain $(AB)(CD)$ and $(AD)(BC)$ similarly. With the identity, these are the twelve elements of T. Note that rotation of the cube by $2\pi/3$ about a diagonal sends T_1 to itself, fixes exactly one vertex of T_1 (since the other fixed vertex is antipodal hence in T_2) and cycles the other three vertices of T_1. Since there are four diagonals, we obtain the four desired 3-cycles in this way.

12.5 Since the icosahedral group contains an element x of order 5, rotation about the center of face F_1 by $2\pi/5$, and an element y of order 2, rotation about the center of edge E_1 by π, we consider the cyclic subgroup generated by xy. This element, hence the associated subgroup will have order 10.

Problems from Chapter 7 of Artin's Algebra.

2.1 a) Let $x = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ in $GL_2(\mathbb{F}_3)$. If $\begin{bmatrix} a & b \\ c & d \end{bmatrix} x = x \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then modulo 3,

$$a \equiv a + c, \quad a + b \equiv b + d, \quad c \equiv c, \quad \text{and} \quad c + d \equiv d.$$

Thus we must have $c \equiv 0 \mod 3$, $a \equiv d \mod 3$, and no restriction on b. Unlike the book's example using $SL_2(\mathbb{F}_3)$ we only need that the determinant of $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \not\equiv 0 \mod 3$.

The centralizer $Z(x) = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} : a \in \{\pm 1\}, b \in \{-1, 0, 1\} \right\}$ has order 6 and thus the order of the conjugacy class $C(x)$ is $|GL_2(\mathbb{F}_3)|/|Z(x)| = (3^2 - 1)(3^2 - 3)/6 = 8$.

b) Let $y = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ in $GL_2(\mathbb{F}_5)$. If $\begin{bmatrix} a & b \\ c & d \end{bmatrix} y = y \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then modulo 5,

$$a \equiv a, \quad 2b \equiv b, \quad c \equiv 2c, \quad \text{and} \quad 2d \equiv 2d.$$

Thus, we must have $b \equiv c \equiv 0$ and $a, d \not\equiv 0$ so that $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{F}_5)$.

The centralizer $Z(y) = \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} : a \in \{1, 2, 3, 4\}, d \in \{1, 2, 3, 4\} \right\}$ has order 16 and thus the order of the conjugacy class $C(y)$ is $|GL_2(\mathbb{F}_5)|/|Z(y)| = (5^2 - 1)(5^2 - 5)/16 = 30$.

2.2 Let $|G| = 21$ and assume that there exists $x \in G$ such that $|C(x)| = 3$. Then $|Z(x)| = |G|/|C(x)| = 7$. Since $x \in Z(x)$, the order of x is 1 or 7. However, if the order of x were one, that would mean that x was the identity, contradicting the fact that $|C(x)| = 3$. Thus $|x| = 7$.

2.3 Let $|G| = 12$ and assume that there exists $x \in G$ such that $|C(x)| = 4$. Then $|Z(x)| = 12/4 = 3$. Since $Z(x)$ contains the center $Z(G)$ as a subgroup, we see that $|Z(G)| = 1$ or 3. Note that element x is not in the center since $|Z(x)| = 3 \neq 1$. However, since $Z(x)$ must contain both $Z(G)$ and x, $|Z(G)| < |Z(x)|$, implying that $|Z(G)| = 1$, hence trivial.

2.7 The first equation $1 + 1 + 1 + 2 + 5$ cannot be the class equation of a group G of order 10 since then $|Z(G)| = 3$ which does not divide $|G|$.

The third equation $1 + 2 + 3 + 4$ cannot be the class equation since then there are conjugacy classes of size 3 and 4, neither of which divide $|G|$.

The fourth equation $1 + 1 + 2 + 2 + 2 + 2$ is impossible, but it is more complicated: if $|G| = 10$ and $x \in G$ has $|C(x)| = 2$, then $|Z(x)| = 5$ which must contain $Z(G)$ as a subgroup. However, $|Z(G)| = 2$ for this class equation, which is a contradiction.

Note: The second equation is possible, in fact it is the class equation of D_5.

2.8 a) For $|G| = 8$, the possible cardinalities of a conjugacy class of such a G are 1, 2, or 4.

We also need a center (i.e. $|Z(G)|$ equals the number of 1's) to be 1, 2, or 4. (Note that non-abelian rules out $1 + 1 + \cdots + 1$.)

Lastly, as we saw above, for any $|C(x)| > 1$ appearing in the class equation, we must have that the value $|Z(G)|$ divides and is strictly less than $|Z(x)| = |G|/|C(x)|$.

Hence, we allow only

$$1 + 1 + 2 + 2 + 2.$$

Note that we disallow 1+1+1+1+4 because for x such that $|C(x)| = 4$, we would have $|Z(x)| = 2 < |Z(G)|$, a contradiction. We also disallow $1 + 1 + 1 + 1 + 2 + 2$ since for x such that $|C(x)| = 2$, we have $|Z(x)| = 4 = |Z(G)|$, another contradiction. Lastly, we disallow $1 + 1 + 2 + 4$ since for x such that $|C(x)| = 4$, we have $|Z(x)| = 2 = |Z(G)|$.

Note: The above sum is the class equation for both the group of quaternions Q_8 and dihedral group D_4. This occurs even though these two non-abelian groups are not isomorphic to one another.

b) For $|G| = 21$ and G non-abelian, the possible cardinalities of a conjugacy class of such a G are 1, 3, or 7. We also need a center of similar sizes. We at first allow

$$1 + 1 + \cdots + 1 + 7 + 7, \quad 1 + 1 + 1 + 3 + 3 + 3 + 3 + 3 + 3, \text{ or } 1 + 3 + 3 + 7 + 7.$$

Then applying analogous logic considering the sizes of the centralizers versus the size of the center, we see that $|G| = 1 + 3 + 3 + 7 + 7$ is the only possibility.

Note: This is the class equation for the subgroup of $GL_2(\mathbb{F}_7)$ generated by $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$.

2.9 a) The class equation for the quaternion group Q_8 is $1 + 1 + 2 + 2 + 2$.

b) The class equation for D_4 is $1 + 1 + 2 + 2 + 2$.

Note: See problem 2.8 (a). Since Q_8 and D_4 are both non-abelian groups of order 8, the above class equation is the only possibility.

To see these more explicitly, if $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ with the relations $i^2 = j^2 = k^2 = -1$ and furthermore $ij = k, ji = -k, jk = i, kj = -i, ki = j$, and $ik = -j$, then the conjugacy classes are

$$Q_8 = \{1\} \cup \{-1\} \cup \{i, -i\} \cup \{j, -j\} \cup \{k, -k\}.$$

For example, $i(j)(-i) = k(-i) = -j$.

Letting $D_4 = \{1, x, x^2, x^3, y, xy, x^2y, x^3y : x^4 = y^2 = 1, yx = x^3y\}$, we get the conjugacy classes

$$D_4 = \{1\} \cup \{x^2\} \cup \{x, x^3\} \cup \{y, x^2y\} \cup \{xy, x^3y\}.$$

For example $yxy^{-1} = yxy = x^3y^2 = x^3$ and $yx^2y = x^2$.

c) The class equation for D_5 is $1+2+2+5$ as mentioned in problem 2.7. In particular,

$$D_5 = \{1\} \cup \{x, x^4\} \cup \{x^2, x^3\} \cup \{y, x^2y, x^4y, xy, x^3y\}.$$

For example $yx^dy^{-1} = x^{-d}$ and $xyx^{-1} = x^2y$, $x(x^2y)x^{-1} = x^4y$, etc.

d) From MT2 Problem 1a (or otherwise), the subgroup $G = T_2(\mathbb{F}_3)$ of invertible upper-triangular matrices in $GL_2(\mathbb{F}_3)$ has cardinality $(3-1)^2 \cdot 3 = 12$. The center of G is $\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \right\}$. Thus for $x \in G \setminus Z(G)$, $|Z(x)|$ is a multiple of 2 dividing $|G|$ which is greater than 2. Thus $|C(x)| = |G|/|Z(x)|$ equals 2 or 3. However, we see that one of the conjugacy classes is of order 3: $\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 0 & 2 \end{bmatrix} \right\}$. Thus the class equation must be

$$|G| = 12 = 1+1+2+2+3+3.$$

If we work explicitly, we will obtain the following decomposition into conjugacy classes:

$$\begin{aligned} T_2(\mathbb{F}_3) \;=\; & \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\} \cup \left\{ \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \right\} \cup \left\{ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \right\} \cup \left\{ \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 0 & 2 \end{bmatrix} \right\} \cup \\ & \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 0 & 2 \end{bmatrix} \right\} \cup \left\{ \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 0 & 1 \end{bmatrix} \right\}. \end{aligned}$$

Answer 2: We see that $T_2(\mathbb{F}_3) \cong D_6$ under the isomorphism $\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} \to \rho$ and $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \to r$

(where $\rho^6 = 1$, $r^2 = 1$, and $r\rho = \rho^{-1}r$). The class equation of D_6 is $1+1+2+2+3+3$, since D_6 decomposes into conjugacy classes as

$$D_6 = \{1\} \cup \{\rho^3\} \cup \{\rho, \rho^5\} \cup \{\rho^2, \rho^4\} \cup \{r, \rho^2 r, \rho^4 r\} \cup \{\rho r, \rho^3 r, \rho^5 r\}.$$

2.14 Let $|G| = 1+4+5+5+5$

a) By the class equation, there exists $x \in G$ such that $|C(x)| = 4$. Then $|Z(x)| = |G|/|C(x)| = 5$, hence there is a centralizer $H = Z(x)$, which is a subgroup of G, of order 5. We claim that H is a normal subgroup.

Lemma: Conjugate elements have the same order.

Proof: If $h^m = 1$ then $(ghg^{-1})^m = gh^mg^{-1} = 1$. Also, if $(ghg^{-1})^n = 1$, then $gh^ng^{-1} = 1$, and thus $gh^n = g$. By the cancellation law, $h^n = 1$ in this case.

If G contains k subgroups of order 5, then G contains $(5-1)k = 4k$ elements of order 5, and they must all be conjugate to one another. However the only proper subsum of $4+5+5+5$ that is divisible by 4 is if $k = 1$. Thus H is the unique subgroup of order 5, hence normal (by Proposition 2.8.18).

b) Since there exists $y \in G$ such that $|C(x)| = 5$, it follows that $K = Z(y)$ is a subgroup of order 4 (by similar reasoning). However, K cannot be normal since a normal subgroup can be partitioned into conjugacy classes and no subsum of $1 + 4 + 5 + 5 + 5$ including 1 (for the identity) equates to 4.

2.17 Assume $|G| = pq$ where p and q are prime and distinct from one another. The possible cardinalities of conjugacy classes are 1, p and q. Also the center is a subgroup of G, so is either of order 1, p, q, or pq.

Case 1) $|Z| = 1$. Then $1 + p + p + \cdots + p \neq pq = |G|$, we must have at least one conjugacy class of size q. Let $x \in G$ have $|C(x)| = q$. Then $|Z(x)| = |G|/|C(x)| = p$ and $Z(x) \cong C_p$. Element $x \neq 1$ since $|C(x)| > 1$ so x must have order p.

Case 2) $|Z| = p$. Then again, G contains a subgroup of order p and therefore an element of order p.

Case 3) $|Z| = q$. Then we have the class equation $= 1 + 1 + \cdots + 1 + p + \cdots + p + q + q + \cdots + q = pq$. Since there are p 1's and p does not divide $(p-1)q$, there must be at least one conjugacy class of size q. We then repeat the argument of Case 1.

Case 4) Finally, if $|Z| = pq$, then G is abelian, and because of its order, must be cyclic. Thus, G contains an element x of order pq and $y = x^q \in G$ has order p.

Note: if G was abelian, $|G| = pq$, and G was not cyclic, then G would contain only non-identity elements of order p and q and they couldn't all be the same order since neither $1 + kp$ nor $1 + kq$ equals pq for any integer k. Thus G would contain an element x of order p and y of order q and therefore $z = xy \in G$ of order pq.

Note that we don't assume any conditions on the relative sizes of p and q so G also contains an element of order q.

3.2 Let Z be the center of G and assume that G/Z is a cyclic group generated by the coset xZ. Assume that $G \neq Z$ so that $x \neq 1$. Then the element $x \in G$ is not in the center so the centralizer $Z(x)$ contains both x and Z. But since G has coset decomposition $G = Z \cup xZ \cup x^2Z \cup \ldots x^{n-1}Z$, the centralizer $Z(x)$ must be all of G. However, this contradicts the fact that $x \notin Z$. We conclude that $G = Z$ under the hypothesis G/Z is cyclic.

3.3 Let $|G| = p^3$ where p is prime and G is non-abelian.

(a) and (b) together) Since $Z(G)$ is a subgroup of G, $|Z(G)| = 1, p, p^2$, or p^3. However, since we assumed G is not abelian, $|Z(G)| \neq p^3$. Furthermore, by Proposition 7.3.1, the center of a p-group cannot be trivial. Hence $|Z(G)| \neq 1$.

Now assume that $|Z(G)| = p^2$. This leads to a contradiction because the centralizer $Z(x)$ of any element $x \in G$ must be a subgroup of G that includes both the center of G and x. Thus, if we pick $x \in G \setminus Z(G)$, we get $|Z(x)| > |Z(G)|$ which means $Z(x) = G$. However, this can only happen if $x \in Z(G)$, so we get a contradiction.

We conclude that the only possibilities are $|Z(G)| = p$ and $|Z(x)| = p^2$ if $x \in G \setminus Z(G)$.

c) For $x \in G$, we have $|C(x)| = |G|/|Z(x)|$ which equals 1 if $x \in Z(G)$ and equals $p = p^3/p^2$ otherwise.

Thus the only possible class equations for a group of order p^3 are $1 + 1 + \cdots + 1 + p + p + \cdots + p$ with p copies of the number one and $(p^2 - 1)$ copies of the number p.

3.4 For $|G| = 8$, if G is abelian, then G either has an element of order eight and $G \cong C_8$, has no element of order eight but has an element of order 4 and $G \cong C_2 \times C_4$, or has no elements of order eight nor four and $G \cong C_2 \times C_2 \times C_2$.

If G is not abelian, by either Problem 2.8 (a) or 3.3 (c), the class equation for G must be $1+1+2+2+2$.

We claim that there are exactly two isomorphism classes for non-abelian groups of order 8, i.e. with this class equation. We proceed as follows:

Label the conjugacy classes as

$$G = \{1\} \cup \{z\} \cup \{x, x'\} \cup \{y, y'\}, \{w, w'\},$$

where the center of G is $\{1, z\}$ and z is of order 2. We first consider the centralizer $Z(x)$. Note that $zx = xz \in Z(x)$ since $(zx)x = xzx = x(zx)$. Thus $Z(x)$ must contain $\{1, z, x, zx\}$. However, $|C(x)| = 2$ implies $|Z(x)| = 4$, and thus the above set is the entire centralizer. Thus x or zx must be the inverse of x.

We also conclude that $zx = x'$, the conjugate of x. Note that otherwise $x' \notin Z(x)$ and we get the equation $(x')(x)(x')^{-1} = x'$ (as the conjugate of x by x' is in $C(x)$ but not x) which implies (by uniqueness of inverses) that $x' = x$, a contradiction. Using analogous logic, we conclude $y' = zy = yz$, and $w' = zw = wz$.

We now have two cases:

Case 1: all elements $g \in \{x, x', y', w, w'\}$ satisfy $g^{-1} = zg$

Case 2: Without loss of generality, y and y' have order 2.

In case 1, we see that all elements of G outside the center have order 4. Thus if we consider the element xy, we get $xy \neq 1, z$. It is clear that $xy \neq 1$ since y is not x's inverse and if $xy = z$ then y would equal the inverse of x', i.e. x, another contradiction. So xy has order 4. However conjugating by (xy) twice fixes any element so $(xy)(xy) = z \in Z(G)$ We conclude that $xy = zy^{-1}x^{-1} = z(zy)(zx) = zyx$. We obtain the rest of the relations among the Quaternion group similarly.

In case 2, we note that if all non-identity elements in a group are order 2, such a G would be abelian. Thus assume that x and $x' = x^{-1}$ are of order 4. We consider the product yx. Note that $yxyx = (yxy^{-1})x = x'x = 1$. Thus yx is of order 2 as well. We note that $yx \neq 1, z, y, y'$ (getting contradictions otherwise). So we assume that $yx = w$ is of order 2 and $y'x = w'$ is also of order 2. Lastly, $(xy)(yx) = x^2 = z$ and so $(yx) = z(xy) = x^3y$. We conclude that G is the Dihedral group D_4 satisfying $x^4 = 1$, $y^2 = 1$, $yx = x^{-1}y$. The extra elements $z = x^2$ and $w = yx$ satisfy the appropriate relations as well. Since there are only two cases for non-abelian groups of order 8, the classification is complete.

4.4 **Lemma:** The Tetrahedral group T is isomorphic to A_4.

Proof: We have already seen from Problem 12.4 of Chapter 6 that T is isomorphic to the index two subgroup of the octahedral group O consisting of rotations stabilizing an inscribed tetrahedron. Since $O \cong S_4$, this means that T is isomorphic to an index two subgroup of S_4. It is possible to see by considering the determinant (i.e. the sign representation) of these rotations stabilizing the tetrahedron that we only get the even permutations.

Proof (version 2): Let T acts faithfully on the four vertices of the tetrahedron. This gives us an injective permutation representation $\phi : T \to S_4$. Furthermore, we can exhibit rotations (as above) that correspond to all eight 3 cycles of S_4. Since these generate A_n for $n \geq 3$, we conclude that Im $\phi = A_4$ and thus $T \cong A_4$.

a) We thus want the class equation of A_4. We see that A_4 consists of an identity element, eight 3-cycles, and three double-transpositions (of order 2). As mentioned above (see Lemma in solution to Problem 2.14 (a) of Chapter 7), conjugate elements have the same order. Thus the conjugacy classes must be refinement of the partition $1+8+3$ noted above. We know that A_4 cannot act transitively on the 3-cycles for instance since 8 does not divide $|A_4| = 12$. We obtain

$$\begin{aligned} A_4 = \{id\} \quad \cup \quad \{(12)(34), (13)(24), (14)(23)\} \quad &\cup \quad \{(123)(4), (142)(3), (134)(2), (243)(1)\} \\ &\cup \quad \{(132)(4), (124)(3), (234)(1), (143)(2)\} \end{aligned}$$

and $|A_4| = 12 = 1+3+4+4$. Note that the second conjugacy class of 3-cycles is obtained by conjugating the first by an odd permutation, i.e. the transposition (12).

b) By the class equation, there exists $x \in T \cong A_4$ such that $|C(x)| = 3$ and $|Z(x)| = 4$. Furthermore, this centralizer can be the only subgroup of size 4 because A_4 contains three elements of order 2 and eight elements of order 3. Thus $Z(x) = \{id, (12)(34), (13)(24), (14)(23)\}$ must be a normal subgroup.

On the other hand, there is no subsum that adds to 6, including 1 (for the identity), thus $T \cong A_4$ contains no normal subgroup of size 6.

4.5 a) We have already seen that $O \cong S_4$ and we know that the class equation of S_4 is

$$|O \cong S_4| = 24 = 1 + 3 + 6 + 6 + 8.$$

b) To find a proper normal subgroup, we consider all the possible subsums of the class equation which includes 1 and divides $|S_4| = 24$. We see that the possible orders for a proper normal subgroup are $1+3 = 4$ or $1 + 3 + 8 = 12$. In particular by joining together the associated conjugacy classes in S_4, we get the two unique proper normal subgroups in S_4. The 3 in the above class equation corresponds to the three double-transpositions. The 8 corresponds to the eight 3-cycles. (Notice that in S_4, these 3-cycles are a single conjugacy class rather than two.) Thus, the normal subgroup of order 4 is $\{1, (12)(34), (13)(24), (14)(23)\}$ and the normal subgroup of order 12 is A_4.

Answer 2: We can also consider O acting on S, the set consisting of pairs of opposite faces, by rotation. In particular, $S = \{(F_1, F_6), (F_2, F_5), (F_3, F_4)\}$. O acts on S transitively and induces a permutation representation $\phi : O \to S_3$. This homomorphism is surjective since all transpositions are obtainable, hence Ker ϕ is a normal subgroup of $O \cong S_4$ of order $|O|/|S_3| = 4$.

Similarly, we let O act on $S' = \{\text{two inscribed tetrahedra}\}$ to induce a surjective permutation representation $\phi' : O \to S_2$ with Ker ϕ' being a normal subgroup of order $|O|/|S_2| = 12$.

It is easiest to use the class equation though to show that these are unique.

Math 5286H: Fundamental Structures of Algebra II

HW 1 Solutions, (February 3rd, 2012)

Problems from Chapter 11 of Artin's Algebra:

1.1 To show that $\alpha = 7 + \sqrt[3]{2}$ is an algebraic number, we use the Binomial Theorem and note that

$$\begin{aligned}(7+\sqrt[3]{2})^3 = 343 + 3\cdot 49\sqrt[3]{2} + 3\cdot 7\sqrt[3]{4} + 2 &= 345 + 147\sqrt[3]{2} + 21\sqrt[3]{4},\\ \text{and } (7+\sqrt[3]{2})^2 &= 49 + 14\sqrt[3]{2} + \sqrt[3]{4}.\end{aligned}$$

Consequently, $\alpha^3 - 21\alpha^2 = -684 - 147\sqrt[3]{2}$, hence

$$\alpha^3 - 21\alpha^2 + 147 - 345 = 0,$$

showing that α is the root of a polynomial with integer entries. We similarly find a polynomial having $\beta = \sqrt{3} + \sqrt{-5}$ as a root. Namely, $\beta^2 = 3 + 2\sqrt{-15} - 5$ and $(\beta^2+2)^2 = -60$. Hence

$$\beta^4 + 4\beta^2 + 64 = 0.$$

Remark: The polynomials $x^3 - 21x^2 + 147x - 345$ and $x^4 + 4x^2 + 64$ are known as *minimal polynomials* (or *irreducible polynomials*) for α and β. We will study these further in Chapter 15.

We will also later see a more general result, which states that the sum of two algebraic numbers is algebraic.

1.3 Since $\mathbb{Q}[\alpha,\beta]$ is a ring containing both α and β, clearly $\gamma = \alpha + \beta \in \mathbb{Q}[\alpha,\beta]$ and we have $\mathbb{Q}[\alpha,\beta] \supseteq \mathbb{Q}[\gamma]$. Furthermore, $\gamma^3 = 2\sqrt{2} + 3(2\sqrt{3}) + 3(3\sqrt{2}) + 3\sqrt{3} = 11\sqrt{2} + 9\sqrt{3} \in \mathbb{Q}[\gamma]$. Thus by taking appropriate $\mathbb{Q}$-linear combinations of γ and γ^3 yields $\sqrt{2}$ and $\sqrt{3}$ by themselves:

$$\frac{1}{2}\gamma^3 - \frac{9}{2}\gamma = \sqrt{2} \quad \text{and} \quad \frac{-1}{2}\gamma^3 + \frac{11}{2}\gamma = \sqrt{3}.$$

Hence we have the other inclusion and we conclude that $\mathbb{Q}[\alpha,\beta] = \mathbb{Q}[\gamma]$. However, these inclusions required rational (not integral) coefficients. We wish to show that there is not a $\mathbb{Z}$-linear combination of powers of γ equal to $\alpha = \sqrt{2}$, i.e. an integer polynomial $g(x) \in \mathbb{Z}[x]$ such that $g(\gamma) = \sqrt{2}$.

The kernel of $\varphi : \mathbb{Z}[x] \to \mathbb{R}$ where $\varphi(x) \mapsto \gamma$ is a principal ideal, namely $(x^4 - 10x^2 + 1)$ using methods similar to Problem 1.1 and Example 11.3.23. Hence $\mathbb{Z}[\gamma] \cong \mathbb{Z}[x]/(x^4 - 10x^2 + 1)$, which means that $\mathbb{Z}[\gamma]$ has $\mathbb{Z}$-basis $\{1, \gamma, \gamma^2, \gamma^3\}$. So if $\alpha \in \mathbb{Z}[\gamma$, then $\alpha = a + b\gamma + c\gamma^2 + d\gamma^3$ for some integers a, b, c, d. However, $\mathbb{Q}[x]/(x^4 - 10x^2 + 1)$ similarly has $\mathbb{Q}$-basis $\{1, \gamma, \gamma^2, \gamma^3\}$, and we already know that $\alpha = \frac{1}{2}\gamma^3 - \frac{9}{2}\gamma$. Thus there cannot be an expression for α involving integer linear combinations of powers of γ. (Note: if there was a higher degree integer polynomial $g(x)$ such that $g(\gamma) = \alpha$, then we can write powers γ^d for $d \geq 5$ also in the basis $\{1, \gamma, \gamma^2, \gamma^3\}$ with integer coefficients, and hence we would again get a integer linear combination of $\{1, \gamma, \gamma^2, \gamma^3\}$ equal to α, a contradiction.) Hence, $\mathbb{Z}[\gamma] \not\supseteq \mathbb{Z}[\alpha, \beta]$ and so $\mathbb{Z}[\gamma] \neq \mathbb{Z}[\alpha, \beta]$.

1.6 (a) Let $S = \{\frac{a}{b} : a, b \in \mathbb{Z}$ and b is not divisible by $3\}$. To show that S is a subring of $\mathbb{Q}$, we note the following: Firstly, $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ (where we then reduce into lowest terms if possible), and if neither b nor d are divisible by 3, then neither is bd. Hence S is closed under addition. Furthermore, $-(\frac{a}{b}) = \frac{-a}{b}$ which is in S when $\frac{a}{b} \in S$. Hence S is closed under additive inverses, i.e. subtraction. S contains the fraction $\frac{1}{1}$, the multiplicative identity. Finally $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$, which again is reduced if possible, and so S is also closed under multiplication.

1.8 (a) The units in $\mathbb{Z}/12\mathbb{Z}$ are $\{1, 5, 7, 11\}$. We note that $1^{-1} = 1$, $5^{-1} = 5$ ($25 \equiv 1 \mod 12$), $7^{-1} = 7$ ($49 \equiv 1 \mod 12$), and $11^{-1} = 11$ ($121 \equiv 1 \mod 12$). The other eight elements are not units since they are a factor of (or share a common factor with) zero, i.e. 12. These are called **zero divisors**.

For instance $\overline{8} \cdot \overline{3} \equiv \overline{0} \mod 12$.

(b) Similarly, the units in $\mathbb{Z}/8\mathbb{Z}$ are $\{1, 3, 5, 7\}$. See part (c) for the proof.

(c) In general, in $\mathbb{Z}/n\mathbb{Z}$, the units are the subset of $\{1, 2, \ldots, n-1\}$ of numbers that are relatively prime to n. Firstly, if $a \in \{1, 2, \ldots, n-1\}$ is not relatively prime to n, i.e. $\gcd(a, n) = d > 1$, then all integral multiples $ka \mod n$ will still be divisible by d. Hence, no such integral multiple ka can be 1. On the other hand, if $\gcd(a, n) = 1$, then there exists $r, s \in \mathbb{Z}$ such that $ra + sn = 1$, i.e. there exists integer r such that $ra \equiv 1 \mod n$. This is the definition of a unit.

1.9 Let $a, b \in R$, we wish to show commutativity of addition. Since R is a ring, it contains a multiplicative identity element 1, and let -1 denote its additive inverse (note that it is possible, e.g. in characteristic 2, that $-1 = 1$ in R). Then by distributivity, $(-1)(b + a) = -b - a$ and by associativity of addition we have

$$(a + b) + (-1)(b + a) = (a + b) + (-b - a) = a + (b - b) + (-a) = a + 0 + (-a) = 0.$$

Hence, $(-1)(b+a)$ is the additive inverse of $(a+b)$ which by uniqueness of inverses implies that $a+b = b+a$, as desired.

3.2 Let I be a nonzero ideal in $\mathbb{Z}[i]$. Then I contains $a + bi$ where $a, b\mathbb{Z}$, not both zero. Since $a - bi \in \mathbb{Z}[i]$, the multiple $(a - bi)(a + bi) = a^2 + b^2$ is also in I. Since at least a or b is nonzero, $a^2 + b^2 \neq 0$ and so I contains a nonzero integer.

3.3 a) The kernel is generated by x and y, i.e. the ideal of bivariate polynomials with trivial constant term.

b) The kernel is generated by x^2-4x+5, which is the lowest degree monic polynomial with real coefficients having $2+i$ as a root. This ideal is principal since $\mathbb{R}[x]$ is a P.I.D.

c) The kernel of the map $\mathbb{Q}[x] \to \mathbb{R}$ is the principal ideal generated by $x^2-2x-1 = (x-1-\sqrt{2})(x-1+\sqrt{2})$. Using the same logic as Example 11.3.23 (i.e. using Lemma 11.3.24), we see that this is also the kernel of the map from $\mathbb{Z}[x] \to \mathbb{R}$.

d) By the same logic as (c), the kernel is the principal ideal generated by $x^4 - 10x^2 + 1$ which equals the product $(x-\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3})$, i.e. the lowest degree monic polynomial with integer coefficients having $\sqrt{2}+\sqrt{3}$ as a root.

e) We see that $y-x^2$ and $z-x^3$ are both in the kernel. We claim that these are in fact the two generators of the kernel. To prove this, we note that if $f(x,y,z) \in K$ (we let K denote the kernel), then by expanding f with respect to powers of z, we obtain $f = a_0(x,y) + a_1(x,y)z + \cdots + a_n(x,y)z^n$, where $a_i(x,y)$ is a polynomial in x and y. Since $z - x^3 \in K$, we can divide $z - x^3$ into f, obtaining

$$f - a_n(z-x^3)^n - (a_{n-1} - nx^3a_n)(z-x^3)^{n-1} - \cdots - a_1'(z-x^3) = b_0(x,y) \in K.$$

We then repeat the argument, dividing $y - x^2$ into $b_0(x,y)$ to get $c_0(x) \in K$. However since $x \mapsto t$, $c_0(x) \in K$ if and only if $c_0(x)$ is the zero polynomial. Thus, we see that any element of K is in fact a linear combination of powers of $(y-x^2)$ and $(z-x^3)$.

For example, the polynomial $z-xy \in (y-x^2, z-x^3)$ since $z-xy = (z-x^3)+(x^3-xy) = (z-x^3)-x(y-x^2)$,

$$\begin{aligned} z^2 - y^3 &= (z-x^3)^2 + (2x^3z - x^6 - y^3) = (z-x^3)^2 + 2x^3(z-x^3) + (x^6 - y^3) \\ &= (z-x^3)^2 + 2x^3(z-x^3) + (y-x^2)^3 + 3x^2(y-x^2)^2 + 3x^4(y-x^2). \end{aligned}$$

3.8 To see that $\phi : R \to R$ defined by $x \mapsto x^p$ is a ring homomorphism when R has prime characteristic p, we note the following.

i) $\phi(x+y) = (x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + \binom{p}{p-1}xy^{p-1} + y^p$. However, p divides $\binom{p}{k}$ as long as $1 \le k \le p-1$ (by logic similar to that of Lemma 7.7.10) since before we reduce to an integer, we note that the numerator of $\binom{p}{k}$ is $p(p-1)\cdots(p-k+1)$ (i.e. divisible by p) while the denominator is $k(k-1)\cdots(1)$ (not divisible by p). Hence in characteristic p, $(x+y)^p$ reduces to $x^p + y^p = \phi(x) + \phi(y)$, sometimes called "The Freshman Dream".

ii) $\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$ follows more easily.

iii) $\phi(1) = 1^p = 1$.

3.9 a) If x is nilpotent, there exists a positive integer n such that $x^n = 0$. Notice that in this case, we use a telescoping sum and obtain $(1+x)(1-x+x^2-x^3+\cdots+(-1)^n x^{n-1}) = 1 \pm x^n = 1$. Hence the element $1+x$ has a multiplicative inverse, and thus is a unit.

b) If R has prime characteristic, with $p \neq 0$, and $a^n = 0$ (since a is nilpotent), then $(1+a)^p = 1 + a^p$ as we saw in Problem 3.8. Repeating this, we see that $(1+a)^{p^m} = 1 + a^{p^m}$ for any nonnegative exponent m. Thus, for some m, $p^m \geq n$ and we obtain $(1+a)^{p^m} = 1 + a^n \cdot a^{p^m - n} = 1$. Thus $1 + a$ is unipotent as desired. There might even be a smallest exponent d such that $(1+a)^d = 1$.

3.12 We verify that $I + J$ is an ideal by verfiying the axioms of Definition 11.3.13. Since I and J are ideals, they are non-empty, so $I + J = \{x + y : x \in I, y \in J\}$ is also non-empty. If $x + y, w + z \in I + J$, then $(x + y) + (w + z) \in I + J$ so $I + J$ closed under addition. Also, if $r \in R$ and $x + y \in I + J$, then $r(x + y) = rx + ry \in I + J$, thus $I + J$ is closed under multiplication by elements in ring R.

3.13 Ideals I of a ring R always contain $0 = 0_R$. (An easy way to see this is that $\alpha - \alpha$ or $O \cdot \alpha \in I$.) Thus $I \cap J$ contains the element 0_R, and hence is non-empty. If $a, b \in I \cap J$, then $a, b \in I$ and $a, b \in J$ so $a + b \in I$ and $a + b \in J$. Thus $a + b \in I \cap J$ and $I \cap J$ is closed under addition. Similarly, $ra \in I$ and $ra \in J$ if $r \in R$ and $a \in I \cap J$, so $I \cap J$ is closed under multiplication by R. We conclude that $I \cap J$ is an ideal.

Here is a counter-example that shows that $\{xy : x \in I, y \in J\}$ (without sums) is *not* an ideal. Let $R = \mathbb{Z}[x]$, $I = J = (x, 2)$. Then $\{ab : a, b \in (x, 2)\}$ contains x^2 and 4 but not $x^2 + 4$.

We next show that the product ideal $IJ = \{\sum xy : x \in I, y \in J\}$ is an ideal: (i) clear that it's non-empty. (ii) sum of a sum is still a sum so closed under addition. (iii) If $r \in R$ and $\sum xy \in IJ$, then $r(\sum xy) = \sum (rx)y \in IJ$ since $x \in I$ implies $rx \in I$.

Lastly, you will prove on the next homework (problem 6.8) that if $I + J = R$, then $IJ = I \cap J$. For example, if $R = \mathbb{Z} = (10) + (21)$, then $(10) \cdot (21) = (10) \cap (21) = (210)$ the ideal generated by the least common-multiple of 10 and 21. However, if $I = (10)$ and $J = (14)$, $(10) \cdot (14) = (140)$ while $(10) \cap (14) = (70)$. In general, $I \cdot J \subset I \cap J$ since $I \cap J$ contains ab where we think of $a \in I$ and $b \in J \subset R$ or $a \in I \subset R$ and $b \in J$.

4.1 Since the homomorphism $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$ such that $\varphi(x) \mapsto 1$ is surjective, the Correspondence Theorem says that ideals in $\mathbb{Z}[x]$ containing the kernel of φ correspond to ideals in $\mathbb{Z}$. In particular, the kernel of φ is the principal ideal $(x - 1)$, and all ideals of $\mathbb{Z}$ are principal of the form (n) where $n \geq 0$.

The ideals in $\mathbb{Z}[x]$ which contain $(x-1)$ are all of the form $I_n = (n, x-1)$ where n is a nonnegative integer. Each corresponds to (n) in the expected way. Ideal I_n can also be thought of as the subset of polynomials $p(x)$ such that the value $p(1)$ is a multiple of n. From this description, it is clear that I_n is the pre-image $\varphi^{-1}(n)$.

Remark: The ideal $(0, x-1) = (x-1)$ and the ideal $(1, x-1) = (1) = \mathbb{Z}[x]$. However for $n \geq 2$, $(n, x-1)$ is not principal. Furthermore, if try to construct another ideal that contains $x - 1$, e.g. $(x - 1, f)$ where $f(x)$ is a polynomial of degree ≥ 1, then we can divide $x - 1$ into f and get a remainder r which is a constant (or 0). It follows that $(x - 1, f) = (r, x - 1)$. Thus, we have described all possible such ideals.

4.2 Similar to Problem 4.1, we consider the homomorphism $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[i]$ such that $\varphi(x) \mapsto i$. This map is surjective and has kernel equal to (x^2+1) since linear factor $(x-i)$ in $\mathbb{C}[x]$ has complex conjugate $(x+i)$. Thus the ideals in $\mathbb{Z}[x]$ containing (x^2+1) correspond to ideals in $\mathbb{Z}[i]$.

In this example, the possible ideals in $\mathbb{Z}[x]$ containing (x^2+1) are (n, x^2+1) where n is a nonnegative integer or $(ax+b, x^2+1)$ where a is positive and $b \in \mathbb{Z}$.

Applying map φ to these ideals, we see the corresponding ideals of $\mathbb{Z}[i]$ are (n), or $(ai+b)$, and hence we see that all ideals in $\mathbb{Z}[i]$ are principal. We will derive this fact in a different way in Chapter 12, hence illustrating why no ideal in $\mathbb{Z}[x]$ containing (x^2+1) needs to have three independent generators.

4.3 a) Writing the ring $R = \mathbb{Z}[x]/(x^2-3, 2x+4)$ as $\mathbb{Z}[x]/I$, we note that I contains $2(x^2-3)-(x-2)(2x+4) = 2$ We then note that the generator $2x+4$ is actually superfluous since $2x+4 = 2(x+2)$. Hence, this ring is really $R = \mathbb{Z}[x]/(x^2-3, 2) = \mathbb{Z}[x]/(x^2+2x+1, 2) \cong \mathbb{F}_2[\alpha]$ where $\alpha = x+1$ satisfies $\alpha^2 = 0$.

b) We studied $\mathbb{Z}[i]/(2+i)$ in class, noting that this ring is $\mathbb{Z}/5\mathbb{Z}$.

c) Let $R = \mathbb{Z}[x]/(6, 2x-1)$ and let $I = (6, 2x-1)$. Note that I also contains $6x - 3(2x-1) = 3$ which makes generator 3 superfluous. Then $I = (3, 2x-1)$, which also contains $3x-(2x-1) = x+1$ and we simplify $I = (3, x+1)$. Hence, $R \cong \mathbb{F}_3[x]/(x+1) \cong \mathbb{F}_3$.

d) Let $R = \mathbb{Z}[x]/(2x^2-4, 4x-5)$ and $I = (2x^2-4, 4x-5)$. Noting that $2(2x^2-4)-x(4x-5) = 5x-8 \in I$ and that $(5x-8)-(4x-5) = x-3 \in I$, we then can divide $2x^2-4$ and $4x-5$ by $x-13$ to obtain $2x^2-4 = (2x+6)(x-3)+14$ and $4x-5 = 4(x-3)+7$. Thus, the integers 7 and 14 are both in I. We thus simplify I to $(7, x-3)$ since we can generate $2x^2-4$ and $4x-5$ from this linear polynomial and the integer 7. In either order we thus kill the transcendental variable x and work mod 7, resulting in $R = \mathbb{F}_7$.

e) Let $R = \mathbb{Z}[x]/(x^2+3, 5)$ and $I = (x^2+3, 5)$. We note that modulo 5, $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 \equiv 4$ and $4^2 \equiv 1$. Thus the quadratic x^2+3 is irreducible modulo 5, and we obtain $R \cong \mathbb{F}_5[x]/(x^2+3) = \{a+b\alpha : a, b \in \mathbb{F}_5, \alpha^2+3 = 0\}$, which is a field of order 25.

5.1 In the ring $\mathbb{Z}[x]/(x^4+x^3+x^2+x+1)$, the product $(\alpha^3+\alpha^2+\alpha)(\alpha^5+1) = \alpha^8+\alpha^3+\alpha^7+\alpha^2+\alpha^6+\alpha = (\alpha^4-\alpha)(\alpha^4+\alpha^3+\alpha^2+\alpha+1)+2\alpha^3+2\alpha^2+2\alpha$. So modulo $f(x) = x^4+x^3+x^2+x+1$, we obtain $2\alpha^3+2\alpha^2+2\alpha$ in the desired basis.

5.4 Determine the ring structure of $R' = \mathbb{Z}[\alpha]$ where

a) $2\alpha = 6, 6\alpha = 15$:

We have $R' \cong \mathbb{Z}[x]/(2x-6, 6x-15)$. We then proceed as in Problem 4.3. Let I be the ideal $(2x-6, 6x-15)$ and note that $3(2x-6)-(6x-15) = 3$ so I contains 3. This makes $6x-15$ a superfluous generator, and we conclude $I = (3, 2x-6) = (3, 2x)$. However, $x = 3(x)-2x$ so $I = (3, x)$ also. We conclude that $R' \cong \mathbb{F}_3$. As a sanity test, note that in $\mathbb{F}_3$, the element $\alpha = 3 = 0_{\mathbb{F}_3}$ satisfies the relation $2\alpha = 6$ and the second relation becomes $0 = 0$.

Remark: Another to think of this problem: we are adding two incompatible relations to $\mathbb{Z}$ which are only solvable if $\alpha = 0$ and $\alpha = 3$. That forces $\mathbb{Z}[\alpha]$ to turn into a ring of characteristic 3, as we saw using the quotient ring construction.

b) $2\alpha - 6 = 0, \alpha - 10 = 0$: We use a similar method, and note that $I = (2x - 6, x - 10)$ simplifies to $(x - 10, 14)$ since $(2x - 6) - 2(x - 10) = 14$. We thus get $R' \cong \mathbb{Z}/14\mathbb{Z}$, modding out by both of these relations.

c) $\alpha^3 + \alpha^2 + 1 = 0, \alpha^2 + \alpha = 0$: Let $I = (x^3 + x^2 + 1, x^2 + x)$. Then I contains $(x^3 + x^2 + 1) - x(x^2 + x) = 1$. Thus I is unit ideal and $R' = \{0\}$.

Math 5286H: Fundamental Structures of Algebra II

HW 2 Solutions, (February 17th, 2012)

Problems from Chapter 11 of Artin's Algebra:

6.2 Yes, $\mathbb{Z}/(6)$ is isomorphic to $\mathbb{Z}/(2)\times\mathbb{Z}/(3)$. Consider the explicit map $\varphi : \mathbb{Z}/(2)\times\mathbb{Z}/(3) \to \mathbb{Z}/(6)$ defined by $\varphi((x+(2))\times(y+(3))) = \overline{3x-2y}+(6)$. This map is a ring homomorphism since φ is clearly compatible with addition and multiplication, and sends $(1+(2))\times(1+(3))$ to $(1+(6))$. We see that it is bijective by computing the image of the six values in $\mathbb{Z}/(2)\times\mathbb{Z}/(3)$, or alternatively exhibiting the explicit inverse map $\varphi^{-1} : \mathbb{Z}/(6) \to \mathbb{Z}/(2)\times\mathbb{Z}/(3)$ defined by $\varphi^{-1}(x+(6)) = (\overline{x}+(2))\times(\overline{x}+(3))$.

On the other hand, $\mathbb{Z}/(8)$ is not isomorphic to $\mathbb{Z}/(2)\times\mathbb{Z}/(4)$. In fact, even forgetting the multiplicative structure, the abelian groups $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ are not isomorphic since the left-hand-side has an element of order 8 but the right-hand-side does not.

Remark: We can also do this problem more quickly using idempotents. In the first case, $S = \mathbb{Z}/(6)$ contains the idempotents $\overline{3}$ and $\overline{4} = \overline{-2}$. (Try squaring them modulo 6 and note that $\overline{4} = \overline{1-3}$.) Thus, $\mathbb{Z}/(6) \cong 3S\times(-2)S$ by Proposition 11.6.2, and we verify that $3S \cong \mathbb{Z}/(2)$ and $(-2)S \cong \mathbb{Z}/(3)$.

In the second case, $\mathbb{Z}/(8)$ has no non-trivial idempotents: $2^2 = 6^2 = 4, 3^2 = 5^2 = 7^2 = 1, 4^2 = 0$, and thus we cannot write $\mathbb{Z}/(8)$ as a product ring.

6.3 We will show that the only ring (using our usual definitions, i.e. commutativity of multiplication and containing an multiplicative identity) of order 10 is the ring $\mathbb{Z}/(10)$.

Firstly note that if $|R| = 10$, then $(R,+)$ is a finite abelian group of order 10. Since 10 is square-free, $(R,+) \cong \mathbb{Z}/10\mathbb{Z}$. Thus the only question is whether R could be given a multiplicative structure different than that of $\mathbb{Z}/(10)$. However, since $(R,+) \cong \mathbb{Z}/10\mathbb{Z}$, we know that the characteristic of R is 10 and thus $\{\overline{0},\overline{1},\overline{2},\ldots,\overline{9}\}$ are all distinct elements. (Here, $\overline{k}$ is shorthand for $1_R+1_R+\cdots+1_R$, as a sum of k terms.) It follows by distributivity that $\overline{a}\cdot\overline{b} = \overline{c}$ where $c = ab = (1+1+1+\cdots+1)(1+1+\cdots+1) \mod 10$, and hence no exotic multiplication structures are possible.

Remark: One might try to break R, a ring of order 10 into product rings using idempotents. In fact, $\mathbb{Z}/(10)$ contains the idempotents $\overline{5}$ and $\overline{6} = \overline{1-5}$. However, this just shows that $\mathbb{Z}/(10) \cong \mathbb{Z}/(2)\times\mathbb{Z}/(5)$ and so there is still only one ring of order 10.

Remark 2: This proof uses the fact that R contains a multiplicative identity 1_R. If we relax this restriction, as is sometimes done in the literature, for instance if one looks at certain matrix rings, then other "rings" of order 10 are possible. For example, $R = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}, \ldots, \begin{bmatrix} 0 & 9 \\ 0 & 0 \end{bmatrix} \right\}$. Note that the product of any two elements in this ring is zero and there is in fact no multiplicative identity.

6.4 (a) $\mathbb{F}_2[\alpha]$, such that $\alpha^2 + \alpha + 1 = 0$, is isomorphic to the quotient ring $\overline{R} = \mathbb{F}_2[x]/(x^2 + x + 1)$. However in $\mathbb{F}_2$, $0^2 + 0 + 1 = 1^2 + 1 + 1 = 1$. Thus $x^2 + x + 1$ has no roots in $\mathbb{F}_2$, hence no linear factors, and hence is irreducible. Consequently $\overline{R} = \{0, 1, \alpha, \alpha + 1\}$ where $\alpha^2 = \alpha + 1$, $(\alpha + 1)^2 = \alpha$, and $\alpha(\alpha + 1) = 1$. Hence $\overline{R}$ is a field of order 4 (every element has a multiplicative inverse).

Remark: We also know from results in Section 11.8 that $(x^2 + x + 1)$ is a maximal ideal of $\mathbb{F}_2[x]$, once we know that it is irreducible, and so we can conclude that $\mathbb{F}_2[x]/(^2+x + 1)$ is a field immediately from this.

(b) We consider $\overline{R} = \mathbb{F}_2[x]/(x^2+1)$. In $\mathbb{F}_2[x]$, the polynomial x^2+1 factors as $(x+1)(x+1)$ since $1^2+1 \equiv 0 \mod 2$ and $x^2+2x+1 \equiv x^2+1 \mod 2$. The ring $\overline{R}$ does not contain any non-trivial idempotents as $\alpha^2 = 1$ and $(\alpha + 1)^2 = 0$. Thus, we simply write this as the four element ring with this funny multiplication. It is isomorphic to $\mathbb{F}_2[\epsilon]$ where $\epsilon^2 = 0$ for what it is worth.

(c) Lastly, we consider $\overline{R} = \mathbb{F}_2[x]/(x^2 + x)$. In $\mathbb{F}_2[x]$, the polynomial $x^2 + x$ factors as $x(x + 1)$ and so $\overline{R}$ contains two non-trivial idempotents as $\alpha^2 = \alpha$ and $(\alpha+1)^2 = \alpha+1$. Hence $\overline{R} \cong \alpha\overline{R} \times (\alpha+1)\overline{R} \cong \mathbb{F}_2 \times \mathbb{F}_2$.

6.5 Adjoining an element α to $\mathbb{R}$ that satisfies the relation $\alpha^2 - 1 = 0$ is equivalent to considering the quotient ring $\overline{R} = \mathbb{R}[x]/(x^2 - 1)$. This example is almost identical to Problem 6.4 (c). We see that $x^2 - 1 = (x - 1)(x + 1)$ and thus R' contains two idempotents, $e = \frac{1}{2}(\alpha + 1)$ and $e' = -\frac{1}{2}(\alpha - 1)$. In particular $\frac{1}{2^2}(\alpha+1)^2 = \frac{1}{4}(\alpha^2+2\alpha+1)$ but if we set $\alpha^2 = 1$, this product becomes $\frac{1}{2}(\alpha+1)$. Note also that $e + e' = 1$. Thus $\overline{R} \cong e\overline{R} \times e'\overline{R}$. The last step is to show that $e\overline{R}$ and $e'\overline{R}$ are each isomorphic to $\mathbb{R}$. But this follows from the fact that in these ideals/subrings, multiplication by α is the same as multiplication by 1 or -1, respectively, and so elements of $e\overline{R}$ or $e'\overline{R}$ are uniquely determined by a choice of a real multiple.

6.7 In $\mathbb{Z}[x]$, the ideal $(2) \cap (x)$ is the set of integer polynomials such that all coefficients are even and with no constant term. The ideal $(2x)$ describes exactly the same set so $(2) \cap (x) = (2x)$.

Consider $f \in \mathbb{Z}[x]$ and divide $2x$ into it to obtain a remainder $\overline{f}$ which has no non-constant terms where the coefficient is not 0 or 1. Also let f_0 denote the constant term of f and write it as $f_0 = 2q_f + r_f$ where $q_f \in \mathbb{Z}$ and $r_f \in \{0, 1\}$. We then have the map $\varphi : \mathbb{Z}[x]/(2x) \to \mathbb{F}_2[x] \times \mathbb{Z}$ defined by $\varphi(\overline{f}) = (\overline{f} - 2q_f, f_0)$. To see that this map is a ring homomorphism, note that $\varphi(\overline{f} + \overline{g}) = (\overline{f} + \overline{g} - 2q_f - 2q_g, f_0 + g_0) = (\overline{f} - 2q_f, f_0) + (\overline{g} - 2q_g, g_0)$, $\varphi(\overline{f} \cdot \overline{g}) = (\overline{fg} - 2q_{fg}, f_0 g_0) = (\overline{f} - 2q_f, f_0) \cdot (\overline{g} - 2q_g, g_0)$ (since the cross-terms vanish mod 2), and finally $\varphi(\overline{1}) = (1, 1)$. This map is not surjective, but it has kernel consisting of polynomials whose constant term is zero (because of the second coordinate) and hence whose higher order coefficients must be zero (because of the first coordinate). Thus φ is injective and $\mathbb{Z}[x]/(2x)$ is isomorphic

to the subring of $\mathbb{F}_2[x] \times \mathbb{Z}$ corresponding to its image. Noting that $(\overline{f} - 2q_f)(0) = f_0$ by construction, we conclude that this image is exactly as described in the book.

6.8 Assume that ideals I and J of R satisfy $I + J = R$.

a) We want to show $IJ = \{\sum a_k b_k : \text{where } a_k \in I \text{ and } b_k \in J\}$ and $I \cap J$ are equal in this case. As we saw in Exercise 3.13 of Chapter 11, $IJ \subset I \cap J$ in all cases since for all $ab \in IJ$, we have $ab \in I$ (thinking of $b \in R$) and $ab \in J$ (thinking of $a \in R$) thus $ab \in I \cap J$. Then since $I \cap J$ is an ideal, any sum $\sum a_k b_k$ will also be in $I \cap J$ since each term is in $I \cap J$.

Hence, it suffices to show that the additional property $I + J = R$ implies the other direction, $I \cap J \subset IJ$.

Note that if $I + J = R$, then there exists $\beta \in I$ and $\gamma \in J$ so that $\beta + \gamma = 1$. Then for any $\alpha \in I \cap J$, we can write $\alpha = \alpha \cdot 1 = \alpha(\beta + \gamma) = \beta\alpha + \alpha\gamma$ where each of these two terms is a product of the form ab where $a \in I$ and $b \in J$. We conclude that $\alpha \in IJ$.

b) We start by considering the map $\varphi : R \to R/I \times R/J$ defined by $\varphi(r) = (r + I, r + J)$. Here we are thinking of elements of R/I and R/J as explicit additive cosets. We can write $\varphi(r+s) = (r+s+I, r+s+J)$, $\varphi(rs) = (r+I, r+J)(s+I, s+J) = (rs+I, rs+J)$, and $\varphi(1) = (1+I, 1+J)$ which is the identity element of the product ring $R/I \times R/J$. (Note that the product $(r+I)(s+I)$ maps to the coset $(rs+I)$.) Thus φ is a ring homomorphism. Its kernel is $I \cap J$ since $\varphi(r) = (0+I, 0+J)$ if and only if $r \in I$ and $r \in J$. Since we assume that $I + J = R$, let $\beta + \gamma = 1$ where $\beta \in I$ and $\gamma \in J$. In this case, $\varphi(\beta) = (0 + I, 1 + J)$ since $\beta = 1 - \gamma$ where $-\gamma \in J$. Similarly, $\varphi(\gamma) = (1 + I, 0 + J)$. Hence φ is surjective, i.e. for any $a + I \in R/I$ and $b + J \in R/J$, we have $\varphi(a\beta + b\gamma) = (a + I, b + J)$. We also saw from part (a) that $I \cap J = IJ$ when $I + J = R$. We conclude by the First Isomorphism Theorem that

$$R/(IJ) \cong R/I \times R/J \quad \text{when} \quad R = I + J.$$

This solves the exercise as well since for any choice of $a + I \in R/I$ and $b + J \in R/J$, there exists an element $x + IJ \in R/IJ$ such that $\varphi(x + IJ) = (a + I, b + J)$. Hence $x \equiv a \mod I$ and $x \equiv b \mod J$.

Remark: We will see a constructive example of the Chinese Remainder Theorem in Problem 1.4 of Chapter 12.

c) In the special case that $IJ = 0$, then the above isomorphism becomes $R/(0) = R \cong R/I \times R/J$.

d) The idempotents are precisely the β and γ described in part (a). See more details below.

Remark: We can also solve parts (c) and (d) together: Let $\beta + \gamma = 1$ as in part (a) since $I + J = R$. If $IJ = 0$, then $1 = 1^2 = (\beta + \gamma)^2 = \beta^2 + \gamma^2$ since the cross-term $2\beta\gamma$ equals zero. Using this, we obtain $\beta^2 = (1 - \gamma^2)$ as $(1 + \gamma)(1 - \gamma) = (1 + \gamma)\beta = \beta + \beta\gamma = \beta$. Similar algebra yields $\gamma^2 = \gamma$. Hence both $\beta \in I$ and $\gamma \in J$ are idempotents and $R \cong \beta R \times \gamma R$. To complete the proof that $R \cong (R/J) \times (R/I)$, we observe that the ideal/subring $\beta R \cong R/J$ since $r\beta \in \beta R$ can be rewritten as $(a + b)\beta$ where $a \in I$ and

$b \in J$. The cross-term $\beta \cdot b = 0$ since $IJ = 0$ and so we are left with a contribution from the quotient R/J. The same argument shows that $\gamma R \cong R/I$.

Example: If we let $R = \mathbb{Z}/(6)$, $I = (2)$ and $J = (3)$, notice that $IJ = (6)$, which is the zero ideal in R. We have $R = I + J$ since $1 \equiv 4 - 3 \mod 6$. We obtain $\mathbb{Z}/(6) \cong R/(2) \times R/(3) \cong \mathbb{Z}/(2) \times \mathbb{Z}/(3)$. If we try the same argument with $R' = \mathbb{Z}/(8)$ and $I' = (2)$, $(J)' = 4$, we still have $I'J' = (0)$ but we do not have $R' = I' + J'$ in this case.

7.1 Let R be a finite integral domain, i.e. a ring with no zero divisors. For every nonzero element $r \in R$, we look at powers r^n and note that since R is finite, $r^d = 1$ for some $d > 0$. Hence $r \cdot (r^{d-1}) = r$ and all nonzero elements of R are units. Thus R is a field.

7.2 Suppose that $R[x]$ is not an integral domain and that $f(x)g(x) = 0$ where $f(x)$ and $g(x)$ are both nonzero. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ where a_n and b_m are both nonzero. Then $f(x)g(x) = 0$ has a term of degree $m + n$, $a_n b_m x^{m+n}$, and so $a_n b_m$ must equal 0. However, a_n and b_m are both nonzero so R cannot be an integral domain. Thus by the contrapositive, $R[x]$ is an integral domain whenever R is. Furthermore, if $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_n \neq 0$ and $n \geq 1$, then $f(x)g(x)$ is a non-constant polynomial, of degree $\geq n \geq 1$, for any $g(x)$. Thus any non-constant polynomial cannot have a multiplicative inverse. Since $R \subset R[x]$, any unit of R is also a unit in $R[x]$, and these are the only units in $R[x]$.

7.3 Any finite integral domain is a field, by Exercise 7.1. Furthermore, by Lemma 3.2.10, the characteristic of a finite field is a prime integer. However, as in Exercise 6.3, for any ring R with 15 elements, $(R, +)$ must be $\mathbb{Z}/15\mathbb{Z}$. But then the characteristic would be 15, which is not prime. Thus, no integral domain with 15 elements exists.

8.2 (a) Since $\mathbb{R}$ is a field, (0) and (1) are only ideals in $\mathbb{R}$. We now consider $\mathbb{R} \times \mathbb{R}$, whose ideals are the products $(0) \times (0)$, $(0) \times (1)$, $(1) \times (0)$, or $(1) \times (1)$. To see that no other ideals are possible, simply note that if I is an ideal of $\mathbb{R} \times \mathbb{R}$ and I contains an element (x, y) whose first coordinate is nonzero, then I also contains $(1, y)$. By similar logic, the second coordinate is either always zero or I contains the element $(0, 1)$ or $(1, 1)$. Since $(1) \times (1)$ is the unit ideal and we have the inclusions $(0) \times (0) \subsetneq (0) \times (1) \subsetneq (1) \times (1)$ and $(0) \times (0) \subsetneq (1) \times (0) \subsetneq (1) \times (1)$, we conclude that the maximal ideals of $\mathbb{R} \times \mathbb{R}$ are $0 \times \mathbb{R}$ and $\mathbb{R} \times 0$.

For (b), (c), and (d), we determine the ideals in a quotient ring by using the Correspondence Theorem.

(b) The ideals in $\mathbb{R}[x]/(x^2)$ are the ideals in $\mathbb{R}[x]$ containing (x^2). Since $\mathbb{R}$ is a field, $\mathbb{R}[x]$ is a Principal Ideal Domain, and the ideals of $\mathbb{R}[x]$ containing (x^2) are (0), (x), and (x^2). By the Correspondence Theorem, we get three ideals in $\mathbb{R}[x]/(x^2)$, the unique maximal ideal being (x).

(c) Analogously, we factor $x^2 - 3x + 2 = (x - 2)(x - 1)$ in $\mathbb{R}[x]$ and we obtain the maximal ideals in $\mathbb{R}[x]/(x^2 - 3x + 2)$ are $(x - 2)$ and $(x - 1)$.

(d) Lastly, we note that x^2+x+1 has non-real roots so is irreducible in $\mathbb{R}[x]$. Hence, $\mathbb{R}[x]/(x^2+x+1)$ is a field where the unique maximal ideal is (0).

8.3 In $\mathbb{F}_2[x]$, the polynomial x^3+x+1 has no roots. In particular, $0^3+0+1 \equiv 1^3+1+1 \equiv 1 \mod 2$. Thus x^3+x+1 has no linear factors and is irreducible so $\mathbb{F}_2[x]/(x^3+x+1)$ is a field.

However, in $\mathbb{F}_3[x]$, the polynomial x^3+x+1 has root 1 since $1^3+1+1 \equiv 0 \mod 3$. Thus $(x-1) \equiv (x+2)$ is a linear factor of x^3+x+1. In fact, x^3+x+1 factors as $(x+2)(x^2+x+2)$ in $\mathbb{F}_3[x]$. (But we do not need the exact factorization.) We conclude that $\mathbb{F}_3[x]/(x^3+x+1)$ has a nontrivial maximal ideal like parts (b) and (c) of the previous problem and hence is not a field.

Problems from Chapter 12 of Artin's Algebra:

1.4 We first note (see Exercise 1.3 of Chapter 12) that the Chinese Remainder Theorem, proven for general ideals in Exercise 6.8, works also in the special case that $R = \mathbb{Z}$. In fact, it was first demonstrated for such examples. (There is also a generalization to more than two ideals as long as each pair I_i, I_j of ideals satisfy $R = I_i + I_j$.) From this theorem, we have the isomorphism $\varphi : \mathbb{Z}/(mn) \to \mathbb{Z}/(m) \times \mathbb{Z}/(n)$ given by $x+(mn) \mapsto (\overline{x}+(m)) \times (\overline{x}+(n))$ when $\gcd(m,n)=1$. We construct the inverse map φ^{-1} by noting that since $\gcd(m,n)=1$, there exist integers r and s so that $rm+sn=1$. We thus let $x=(sn)a+(rm)b$ and obtain $x \equiv a \mod m$ and $x \equiv b \mod n$. Having outlined the general procedure, we now apply it to the examples.

(a) If $x \equiv 3 \mod 8$ and $x \equiv 2 \mod 5$, we notice $\gcd(8,5)=1$, and in particular $2 \cdot 8 - 3 \cdot 5 = 1$. So let $x = 3(-15)+2(16) = -13 \equiv 27 \mod 40$. We indeed verify that $27 \equiv 3 \mod 8$ and $27 \equiv 2 \mod 5$.

Remark: This might also be found by inspection by looking at the intersection of the sets $\{3,11,19,27,35\}$ and $\{2,7,12,17,22,27,32,37\}$.

(b) We do this problem in two steps since there are three congruences. First we find $y \mod 120$ so that $y \equiv 3 \mod 15$ and $y \equiv 5 \mod 8$ ($120 = 15 \cdot 8$). With the same method, we see $\gcd(8,15)=1$, and it is easy to eyeball $2 \cdot 8 - 1 \cdot 15 = 1$. So we let $y \equiv 3(16)+5(-15) \equiv 93 \mod 120$. Next we wish to find $x \mod 840$ so that $x \equiv 93 \mod 120$ and $x \equiv 2 \mod 7$. We see $\gcd(120,7)=1$ and $1 \cdot 120 - 17 \cdot 7 = 1$. (This is still easy to spot but otherwise there is the extended Euclidean algorithm, which we have not discussed in class, that can be used to find r and s.) So we choose $x \equiv 2(120)+93(-119) \equiv -10827 \equiv 93 \mod 840$. Actually, the fact that x and y both equal 93 is a coincidence since $93 \equiv 2 \mod 7$. So if we would have checked all the congruences at that point instead of continuing we would have had a pleasant surprise.

(c) Again $\gcd(43,71)=1$, and we do an adhoc version of the extended Euclidean algorithm:

$$71 = 1 \cdot 43 + 28, \quad 43 = 1 \cdot 28 + 15, \quad 28 = 1 \cdot 15 + 13, \quad 15 = 1 \cdot 13 + 2, \quad 13 = 6 \cdot 2 + 1.$$

Thus we can back-solve, and obtain

$$1 = 13 - 6\ddot{2} = 13 - 6 \cdot (15-13) = -6 \cdot 15 + 7 \cdot 13 = -6 \cdot 15 + 7(28-15) = -13 \cdot 15 + 7 \cdot 28.$$

Continuing, $1 = -13(43-28) + 7\cdot 28 = 20\cdot 28 - 13\cdot 43 = 20(71-43) - 13\cdot 43 = 20\cdot 71 - 33\cdot 43$.

Thus if we want $x \equiv 13 \mod 43$ and $x \equiv 7 \mod 71$, we take $x \equiv 13(20\cdot 71) + 7(-33\cdot 43) \equiv 2421 \mod 3053$ where $3053 = 43\cdot 71$. Like magic, you can verify that $x = 2421$ satisfies the desired congruences.

2.1 (a) Since $x^3 + x^2 + x + 1$ is a cubic, we look for possible roots in $\mathbb{F}_2$. We see $0^3 + 0^2 + 0 + 1 \equiv 1 \mod 2$ and $1^3 + 1^2 + 1 + 1 \equiv 0 \mod 2$. Thus $(x-1) \equiv (x+1)$ is a root. By synthetic division, we obtain $x^3+x^2+x+1 = (x+1)(x^2+1)$. We see that 1 is again a factor of x^2+1, and in fact $x^3+x^2+x+1 = (x+1)^3$ in $\mathbb{F}_2[x]$. This can also be done by inspection and using the Binomial Theorem to expand this cube.

(b) We again try to find roots, this time in $\mathbb{F}_5$. By inspection, $1^2 - 3 - 3 \equiv 0 \mod 5$ and so $(x-1)$ is a linear factor. We obtain $x^2 - 3x - 3 = (x-1)(x-2)$ in $\mathbb{F}_5$.

(c) We attempt to find a square-root of $-1 \equiv 6$ in $\mathbb{F}_7$. We see that no such root of x^2+1 exists, hence x^2+1 is irreducible in $\mathbb{F}_7[x]$.

2.3 This is similar to Monday's question about $x^2 - 1$ in class. By trying out $0, 1, 2, \ldots, 7$ we see that the polynomial $x^2 - 2$ has no roots in $\mathbb{Z}/(8)[x]$. Note that it is actually sufficient to test $0, 1, 2, 3, 4$ since $5, 6, 7$ are equivalent to $-3, -2, -1$. A similar shortcut holds for part (c) of the previous problem.

2.6 (a) We wish to show that $\mathbb{Z}[\omega]$ (with $\omega = e^{2\pi i/3}$) is a Euclidean Domain with the size function $\sigma(a+b\omega) = a^2 - ab + b^2$ when a and b are not simultaneously zero. Note that as a complex number, $\omega = \frac{-1+\sqrt{-3}}{2}$, and if we think of $\alpha = a + b\omega$ as a complex number, then $\sigma(\alpha) = |\alpha|^2 = \alpha\overline{\alpha} = (a - \frac{b}{2})^2 + (\frac{b\sqrt{3}}{2})^2$.

We use the fact that ω is a primitive cube root of unity to see that each principal ideal $(\alpha) \subset \mathbb{Z}[\omega]$ is a triangular lattice. (As opposed to $\mathbb{Z}[i]$ where the fundamental regions of the lattice were squares instead.) In particular, we see that α, $\omega\alpha$, and $\omega^2\alpha$ are all elements of $\mathbb{Z}[\omega]$. Furthermore, since $x^3 - 1$ factors as $(x-1)(x^2+x+1)$ and $\omega \neq 1$ is a root of $x^3 - 1$, we have the identity $\omega^2 + \omega + 1 = 0$. (This identity can also be proven explicitly using $\omega^2 = \frac{-1-\sqrt{-3}}{2}$.) Thus $\alpha + \omega\alpha + \omega^2\alpha = 0$, hence why we get triangles as fundamental regions, in fact equilateral triangles. (This is similar to $\mathbb{Z}[i]$ where $1 + i + (-1) + (-i) = 0$ and so the fundamental regions have four sides and are squares.)

The centroid of an equilateral triangle (with side lengths $|\alpha|$ is at most a squared distance of $\frac{1}{3}|\alpha|^2 = \frac{1}{3}\sigma(\alpha)$ away from a lattice point, i.e. multiple of α. (This is done using 30-60-90 triangles to calculate the lengths of the segments in the associated barycentric subdivision.) So if we write $\beta = \alpha q + r$, we get $\sigma(r) \leq \frac{1}{3}\sigma(\alpha) < \sigma(\alpha)$ unless $r = 0$.

Answer 2: One can also do the division more explicitly by considering β/α in $\mathbb{Q}[\sqrt{-3}]$ and then finding the nearest element of $\mathbb{Z}[\omega]$ whose two components are half-integers satisfying a parity contraint. Some crude bounds give that the remainder has the form $\frac{2r_0+r_1}{2} + \frac{r_1}{2}\sqrt{-3}$, where $|r_0| \leq \frac{1}{4}$ and $|r_1| \leq \frac{1}{2}$. Thus $\sigma(r) \leq \frac{1}{4}\sigma(\alpha) + \frac{3}{16}\sigma(\alpha) = \frac{7}{16}\sigma(\alpha)$ when $r \neq 0$.

(b) The case of $\mathbb{Z}[\sqrt{-2}]$ more closely mimics our proof in $\mathbb{Z}[i]$ using square lattices. We wish to show that the size function $\sigma(a+b\sqrt{-2}) = a^2+2b^2$, which is again $|\alpha|^2$ if $\alpha = a+bi\sqrt{2}$, leads to a division algorithm which terminates. Notice that for $\alpha \in \mathbb{Z}[\sqrt{-2}]$, the principal ideal (α) is again a lattice, only this time the fundamental domains are rectangles where one side has length $|\alpha|$ and the other one has size $|\alpha|\sqrt{2}$. For all $\beta \in \mathbb{Z}[\sqrt{-2}]$, $\beta - q\alpha = r$ is either zero or $\sigma(r)$ is at most $(\frac{1}{2})^2 + 2(\frac{1}{2})^2 = \frac{3}{4}|\alpha|^2 = \frac{3}{4}\sigma(\alpha)$.

3.1 (a) By applying the automorphism $\sqrt{2} \to -\sqrt{2}$ in $\mathbb{R}$ which acts trivially in $\mathbb{Z}[x]$, we get that the polynomial $(x-1-\sqrt{2})(x-1+\sqrt{2}) = x^2-2x-1$ is in the kernel of $\varphi : \mathbb{Z}[x] \to \mathbb{R}$ sending x to $1+\sqrt{2}$. Futhermore, x^2-2x-1 is primitive and irreducible in $\mathbb{Q}[x]$, so x^2-2x-1 is a prime element of the Unique Factorization Domain $\mathbb{Z}[x]$. If the kernel of φ containing another element, call it $f(x)$, then we could divide $f(x)$ by x^2-2x-1 and obtain a linear integer polynomial or constant as a remainder. Thus without loss of generality, consider $f(x) = ax+b$ where $a, b \in \mathbb{Z}$, $a = 0$ allowed. Then $\varphi(f) = a + a\sqrt{2} + b \neq 0$ unless $a = 0$ and $b = 0$. Thus the kernel of φ is a principal ideal with the named prime element as a generator.

(b) By similar logic, we try to find an element of the kernel of φ which sends x to $\frac{1}{2}+\sqrt{2}$. To make this easier, we first think of φ of sending $\mathbb{Q}[x]$ to $\mathbb{R}$, and obtain element of the kernel $(x-\frac{1}{2}-\sqrt{2})(x-\frac{1}{2}+\sqrt{2}) = x^2-x-\frac{7}{4}$. This element of $\mathbb{Q}[x]$ can be written as $\frac{1}{4}(4x^2-4x-7)$ where $4x^2-4x-7$ is the unique primitive integer polynomial in such a factorization. Thus $4x^2-4x-7$ is a prime element of $\mathbb{Z}[x]$ that is in the kernel of φ.

We apply Theorem 12.3.6 (a) here to show that the kernel is again principal. Suppose that $f(x)$ is another element in the kernel that is not a multiple of $4x^2-4x-7$. But $\mathbb{Q}[x]$ is a principal ideal domain and so thinking of them as polynomials with rational coefficients, we have that $f(x)$ must be a multiple of $4x^2-4x-7$ in $\mathbb{Q}[x]$. However, since $4x^2-4x-7$ is a primitive polynomial, $4x^2-4x-7$ must therefore divide $f(x)$ in $\mathbb{Z}[x]$ as well.

3.2 Suppose that two polynomials, f and g, in $\mathbb{Z}[x]$ are relatively prime elements of $\mathbb{Q}[x]$. Since $\mathbb{Q}[x]$ is of the form $F[x]$, with F a field, it is a Principal Ideal Domain and relatively prime means that $\gcd(f,g) = 1$. Thus there exists $r(x)$ and $s(x) \in \mathbb{Q}[x]$ so that $r(x)f + s(x)g = 1$. However we multiply through by a common integer d to clear denominators in $r(x)$ and $s(x)$, obtaining $r'(x)$ and $s'(x) \in \mathbb{Z}[x]$ so that $r'(x)f + s'(x)g = d$. Thus the ideal (f,g) contains the integer d in $\mathbb{Z}[x]$ and we obtain the forward direction.

To see the reverse direction, assume that the ideal (f,g) contains the integer d. Then there exists $r'(x)$ and $s'(x) \in \mathbb{Z}[x]$ such that $r'(x)f + s'(x)g = d$, and dividing by d, we obtain $r(x)f + s(x)g = 1$ as above. Hence f and g are relatively prime in $\mathbb{Q}[x]$, completing the proof.

Math 5286H: Fundamental Structures of Algebra II

HW 3 Solutions, (March 9th, 2012)

Problems from Chapter 13 of Artin's Algebra:

1.1 Yes, $\alpha = \frac{1}{2}(1+\sqrt{5})$ is an algebraic integer since it is a root of $x^2 - x - 1 = (x-\alpha)(x+\alpha-1)$.

3.2 To check whether the following lattices of integer linear combinations are ideals, we must multiply each element of the lattice basis $\mathbf{B}$ by $\delta = \sqrt{-5}$ and try to rewrite the result as an integer linear combination of $\mathbf{B}$. We do not need to check closure under multiplication by any other element of $\mathbb{Z}[\sqrt{-5}]$ since the lattices are already closed under integer linear combinations.

(a) $5\delta = 5(1+\delta) - 1(5)$ but $\delta(1+\delta) = \delta - 5 \neq 5a + (1+\delta)b$ for any integers a and b. Otherwise, we would need $5a + b = -5$ and $b = 1$, which has no integer solutions. Thus, $\mathbf{B}$ is not an ideal in this case.

(b) $7\delta = 7(1+\delta) - 1(7)$ but again $\delta - 5 = 7a + (1+\delta)b$ has no integer solutions, and $\mathbf{B}$ is not an ideal in this case either.

4.1 Let $\delta = \sqrt{-6}$, $A = (2, \delta)$, $B = (3, \delta)$. The product ideal $AB = (6, 2\delta, 3\delta, -6)$. We note that δ divides each of these four terms and $\delta = 3\delta - 2\delta$ so $\delta \in AB$ also. Thus $AB = (\delta)$ is an ideal.

A lattice basis for AB (so that elements are integer linear combinations) is given by $\{\delta, -6\}$, where $-6 = \delta \cdot \delta$. Equivalently, we could use $\{\delta, 6\}$ as our lattice basis, or any other $\mathbb{Z}$-spanning and $\mathbb{Z}$-linearly independent set.

5.1 (a) To verify whether (11) is a prime ideal in $\mathbb{Z}[\sqrt{-5}]$, we check whether or not $x^2 + 5$ is irreducible in $\mathbb{F}_{11}[x]$. In particular, $\mathbb{F}_{11}$ does not contain a square-root of -5 so (11) is indeed prime.

(b) The ideal $(14) = (2)(7)$ and so we now check, the same way as in part (a), whether (2) or (7) are prime ideals in $\mathbb{Z}[\sqrt{-5}]$.

$x^2 + 5$ factors as $(x+1)(x+1)$ in $\mathbb{F}_2[x]$, so (2) is not prime. In particular, $(2) = (2, 1+\sqrt{-5})(2, 1-\sqrt{-5})$ as we saw in class and in the text.

$x^2 + 5$ factors as $(x+3)(x+4)$ in $\mathbb{F}_7[x]$, so (7) is also not prime. We must try to factor (7) into the form $(a, b+c\sqrt{-5})(a, b-c\sqrt{-5})$ for integers a, b, and c. In fact, we can utilize the fact that $(x+3)$ is a factor of x^2+5 in $\mathbb{F}_7[x]$ to see that $\overline{x+3} = 3 + \sqrt{-5}$ is a zero divisor in $\mathbb{Z}[\sqrt{-5}]/(7)$. In particular, we obtain

$P\overline{P} = (7, 3+\sqrt{-5})(7, 3-\sqrt{-5}) = (49, 21+7\sqrt{5}, 21-7\sqrt{5}, 14) = (7)$ as 7 divides each generator and $49 - 3 \cdot 14 = 7 \in P\overline{P}$. We know that P and $\overline{P}$ are prime since their norms are prime integers.

We conclude that (14) factors into prime ideals as $(2, 1+\sqrt{-5})(2, 1-\sqrt{-5})(7, 3+\sqrt{-5})(7, 3-\sqrt{-5})$.

5.2 (a) Let $\delta = \sqrt{-3}$ and A be the ideal $(2, 1+\delta)$ of $R = \mathbb{Z}[\delta]$.

Then the quotient ring R/A is isomorphic to $\mathbb{Z}[x]/(x^2+3, 2, 1+x) \cong \mathbb{F}_2[x]/(x+1) \cong \mathbb{F}_2$ since $x^2+3 \equiv x^2+2x+1$ is a multiple of $x+1$ modulo 2.

Since this quotient ring R/A is a field, i.e. $\mathbb{F}_2$, we conclude that A is a maximal ideal.

(b) $A\overline{A} = (4, 2+2\delta, 2-2\delta, 4) = (4, 2+2\delta)$. Since the product ideal $A\overline{A}$ is self-conjugate, if it was principal, it would have to be generated by a positive integer. We note that both of these generators have a norm of 16, so 4 would be the generator in this case. However, $2+2\delta$ is not divisible by 4. Thus the ideal $A\overline{A}$ is not principal, showing that the Main Lemma (Lemma 13.4.8) does not hold for this subring of a ring of integers.

(c) The ideal A contains the principal ideal (2) since 2 is a generator of both ideals. However, A does not divide (2). To see this, we note that if $\alpha \in B$ and $AB = (2)$ then 2 must divide every generator of AB, i.e. $\alpha(1+\delta)$. However $N(2) = 4 = N(1+\delta)$, so $N(\alpha) = 1$. Since we are in $\mathbb{Z}[\sqrt{-3}]$ instead of $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, we note that the only elements of norm 1 are ± 1 (See Propostiion 13.2.2). Since $2 \neq \pm(1+\sqrt{-3})$, we conclude that $AB \neq (2)$ for any B.

6.1 Let $d = -14$.

Consider $p = 2$. The polynomial x^2+14 factors in $\mathbb{F}_2[x]$ as $x \cdot x$ so (2) splits and ramifies in $\mathbb{Z}[\sqrt{-14}]$. We see that $(2) = (2, \sqrt{-14})^2$ and $\{2, \sqrt{-14}\}$ is a lattice basis for one of these two prime ideals. (To see this is a lattice basis, we note that $2\sqrt{-14}$ is in the span of the basis, as is $\sqrt{-14}\sqrt{-14} = -14$. Then using integer linear combinations, we can obtain all other elements of the ideal.)

Next, $p = 3$. The polynomial x^2+14 factors in $\mathbb{F}_3[x]$ as $(x+7) \cdot (x+2)$ so (3) splits in $\mathbb{Z}[\sqrt{-14}]$. Specifically, $(3) = (3, 2+\sqrt{-14})(3, 1+\sqrt{-14})$, reading this off of the factorization of x^2+14 modulo 3. (Let us prove that $\{3, 2+\sqrt{-14}\}$ is a lattice basis for the first prime ideal: $3\sqrt{-14} = -2(3)+3(2+\sqrt{-14})$ and $(2+\sqrt{-14})\sqrt{-14} = -6(3)+2(2+\sqrt{-14})$.)

Next, $p = 5$. The polynomial x^2+14 factors in $\mathbb{F}_5[x]$ as $(x+14) \cdot (x+1)$ so (5) splits in $\mathbb{Z}[\sqrt{-14}]$. We obtain $(5) = (5, 1+\sqrt{-14})(5, 4+\sqrt{-14})$, and $\{5, 1+\sqrt{-14}\}$ is a lattice basis for the first prime ideal. (Proof as above.)

Next, $p = 7$. The polynomial x^2+14 factors in $\mathbb{F}_7[x]$ as $x \cdot x$ so (7) splits and ramifies in $\mathbb{Z}[\sqrt{-14}]$. We obtain $(7) = (7, \sqrt{-14})^2$ and this prime ideal has lattice bais $\{7, \sqrt{-14}\}$. (Proof as above.)

Next, $p = 11$. The polynomial $x^2 + 14$ is irreducible in $\mathbb{F}_{11}[x]$ since there is no square-root of $-14 \equiv -3$ in $\mathbb{F}_{11}[x]$. Thus (11) remains prime in $\mathbb{Z}[\sqrt{-14}]$. (Though not necessary to write, the lattice basis for prime ideal (11) is $\{11, 11\sqrt{-14}\}$.)

Finally, $p = 13$. The polynomial $x^2 + 14$ factors in $\mathbb{F}_{13}[x]$ as $(x + 5)(x + 8) \cdot x$ so (13) splits in $\mathbb{Z}[\sqrt{-14}]$. We obtain $(13) = (13, 5 + \sqrt{-14})(13, 8 + \sqrt{-14})$ and $\{13, 5 + \sqrt{-14}\}$ is a lattice basis for the first prime ideal. (Proof as above.)

Remark: The ideals $(p, a+\sqrt{-d})$ appearing above always have as $\{p, a+\sqrt{-d}\}$ as lattice bases in $\mathbb{Z}[\sqrt{-d}]$ since $p(\sqrt{-d}) = -a(p) + p(a + \sqrt{-d})$ and $(a + \sqrt{-d})\sqrt{-d} = q(p) + a(a + \sqrt{-d})$. Here we must solve for q so that $pq + a^2 = -d$, but this has a solution since a is a solution to $x^2 + d \equiv 0 \mod p$.

6.3 (a) If p, an integer prime, remains prime in R, then (p) is a prime ideal, and by Lemma 13.5.4 (d), (p) is a maximal ideal. Consequently, $R/(p)$ is a field. Furthermore, we can rewrite $R/(p)$ as $\mathbb{Z}[x]/(x^2 + d, p) \cong \mathbb{F}_p[x]/(x^2 + d)$. Since $R/(p)$ is a field, so is $\mathcal{F} = \mathbb{F}_p[x]/(x^2 + d)$, and $x^2 + d$ is irreducible. Thus there are p^2 elements of $\mathcal{F}$, i.e. of the form $ax + b$ where $a, b \in \mathbb{F}_p$.

(b) In this case that p splits but does not ramify, then $R/(p) \cong \mathbb{F}_p[x]/(x^2 + d)$ where $x^2 + d$ factors as $(x - a)(x - b)$ in $\mathbb{F}_p[x]$ where $a \neq b$. In this case, there are again p^2 elements in $\mathbb{F}_p[x]/(x^2 + d)$, and we can factor the ideal $(x^2 + d)$ into the product ideal IJ where $I = (x - a)$ and $J = (x - b)$. Notice that $(x-a)-(x-b) = b-a \neq 0 \in \mathbb{F}_p$ is in $I+J$, so $I+J = (1)$. Thus the Chinese Remainder Theorem applies, see Chapter 11, Problem 6.8 from HW 2, and we obtain $R/(p) \cong R/I \times R/J$.However, $|R/(p)| = p^2$ so $|R/I| = |R/J| = p$ (since they both have cardinality > 1) and thus $R/I \cong R/J \cong \mathbb{F}_p$ as desired.

Remark 1: For a more concrete proof, we use the fact that there exists $c \in \mathbb{F}_p^\times$ such that $c(x-a)-c(x-b) = c(b - a) = 1$ and so in $R/(p)$, we have $\beta = c(\sqrt{-d} - a)$ is an idempotent by Problem 6.8 (d) of Chapter 11, as is $1 - \beta$. Letting $S = R/(p)$, we obtain, $S \cong \beta S \times (1 - \beta)S$, and each subring has cardinality p.

Remark 2: We wrote the above proofs as if $d \equiv 2, 3 \mod 4$, but replacing $x^2 - d$ with $x^2 - x + \frac{1-d}{4}$, the proof follows analogously.

7.1 If $R = \mathbb{Z}[\sqrt{-5}]$ and $B = (3, 1 + \sqrt{-5})$, then $B^2 = (9, 3 + 3\sqrt{-5}, -4 + 2\sqrt{-5})$. We note that the norms of these three generators are 81, 54, and 36, respectively. Since the greatest common divisor of these three integers is 9, that implies that the principal ideal B^2 is generated by an element of norm 9. (Note that we know that B^2 is principal as the Class Group of $\mathbb{Z}[\sqrt{-5}]$ is cyclic of order 2.)

We thus write down all elements of $\mathbb{Z}[\sqrt{-5}]$ with norm 9: either ± 3 or $\pm 2 \pm \sqrt{-5}$. The integer 3 does not divide $-4 + 2\sqrt{-5}$. However $\alpha = -2 + \sqrt{-5}$ does. In fact $9 = (-2 + \sqrt{-5})(-2 - \sqrt{-5})$ and $3 + 3\sqrt{-5} = (-2 + \sqrt{-5})(1 - \sqrt{-5})$, so α divides all three generators of B^2. Additionally, we have the linear combination $\alpha = (3 + 3\sqrt{-5}) - (-4 + 2\sqrt{-5}) - 9 \in B^2$, finishing the proof that $B^2 = (\alpha)$.

7.4 Let $\delta = \sqrt{-6}$ and $R = \mathbb{Z}[\delta]$.

(a) First of all, both of these lattices, $(2,\delta)$ and $(3,\delta)$, are in fact ideals trivially. (Since 2δ (resp. 3δ) and -6 are integer linear combinations of 2 (resp. 3) and δ.)

Since $(2,\delta)(2,-\delta) = (4, \pm 2\delta, -6) = (2)$ and $(3,\delta)(3,-\delta) = (9, \pm 3\delta, -6) = (3)$, both of these ideals have a norm that is a prime integer and hence are prime ideals.

Answer 2: We could also consider the quotient rings $\mathbb{Z}[x]/(x^2+6, 2, x) \cong \mathbb{F}_2$ and $\mathbb{Z}[x]/(x^2+6, 3, x) \cong \mathbb{F}_3$ respectively. Since they are fields, $(2,\delta)$ and $(3,\delta)$ are maximal, hence prime, ideals.

Remark: As we will see in part (c), the class group has order 2 in this case, so even though $(2,\delta)$ and $(3,\delta)$ are both prime, they are actually in the same ideal class.

In particular, $(3,\delta) = \lambda \cdot (2,\delta)$ where $\lambda = \frac{1}{2}\delta \in \mathbb{C}$.

(b) $(6) = (2)(3) = (2,\delta)^2(3,\delta)^2$. Notice that both primes 2 and 3 ramify, i.e the prime ideals in part (a) are self-conjugate.

(c) It was mentioned in lecture that the class group of $R = \mathbb{Z}[\sqrt{-6}]$ is cyclic of order 2. This follows from Theorem 13.7.10, which states that the class group is generated by the classes of prime ideals P, whose norms are prime integers $p \leq \mu$. For $d = -6$, by equation (13.7.7), $\mu = 2\sqrt{6/3} = 2\sqrt{2} \approx 2.824\ldots$.

Consequently, it suffices to find all prime ideals P, whose norm is 2, i.e. satisfying $P\overline{P} = (2)$. We consider x^2+6 in $\mathbb{F}_2[x]$, noting, that this polynomials splits and ramifies. Consequently, (2) splits and in fact $(2) = A^2$ where $A = (2,\delta) = \overline{A}$. This is unique factorization of (2) into prime ideals, so no other prime ideal except $(2,\delta)$ has norm 2. We conclude that the class group has a single generator, and hence must be cyclic of order 2.

Remark: Notice also that $A^2 = (4, 2\delta, -6) = (2)$, which is in the same similarity class as the unit ideal.

Problems from Chapter 15 of Artin's Algebra:

2.1 The element $\alpha \in \mathbb{C}$ satisfies $x^3 - 3x + 4$. We wish to find $\beta = (c\alpha^2 + b\alpha + a)$ such that

$$(\alpha^2 + \alpha + 1)\beta = 1 + (\alpha^3 - 3\alpha + 4)\gamma = 1 + 0.$$

Since β is of degree 2, this implies $\gamma = e\alpha + d$ must be of degree 1. We thus solve for a, b, c, d, e so that

$$c\alpha^4 + (b+c)\alpha^3 + (a+b+c)\alpha^2 + (a+b)\alpha + a = e\alpha^4 + d\alpha^3 - 3e\alpha^2 + (4e-3d)\alpha + (4d+1).$$

Thus $c = e, b + c = d, a + b + c = -3e, a + b = 4e - 3d$, and $a = 4d + 1$. We solve this linear system involving five variables and five unknowns to conclude $\beta = -\frac{3}{49}\alpha^2 - \frac{5}{49}\alpha + \frac{17}{49}$ and $\gamma = -\frac{3}{49}\alpha - \frac{8}{49}$. Hence $\beta \in \mathbb{Q}$ is the inverse of $\alpha^2 + \alpha + 1$.

2.2 Since α is a root of $f(x)$, we have $\alpha^n - a_{n-1}\alpha^{n-1} + \cdots + (-1)^n a_0 = 0$. Since f is irreducible, $a_0 \neq 0$. Consequently, we get the identity $\alpha^n - a_{n-1}\alpha^{n-1} + \cdots + (-1)^{n-1}a_1\alpha = (-1)^{n-1}a_0$, which we can rewrite as

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

We conclude that $\alpha^{-1} = (-1)^{n-1}\frac{1}{a_0}\alpha^{n-1} + (-1)^{n-2}\frac{a_{n-1}}{a_0}\alpha^{n-2} + \cdots + \frac{a_1}{a_0}$.

3.2 Let us first show that $f = x^4 + 3x + 3$ is irreducible over $\mathbb{Q}$. We notice that $p = 3$ divides all non-leading terms and yet p^2 does not divide the constant term. Hence, by the Eisenstein criterion, f is irreducible.

Remark: One also might start with the rational root test, i.e. plugging in ± 1 or ± 3, to see that f has no rational roots. However, then there is extra work to show that f cannot factor into two quadratics.

We next let α be a root of f in a splitting field (or a complex number α satisfying this polynomial in this case), and construct the tower

$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \alpha)$ and $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt[3]{2}, \alpha)$.

Since $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ are relatively prime, the total degree $[\mathbb{Q}(\sqrt[3]{2}, \alpha) : \mathbb{Q}] = 12$ and we conclude that the degree of α over $\mathbb{Q}(\sqrt[3]{2})$ is also 4. Hence $x^4 + 3x + 3$ is irreducible over $\mathbb{Q}(\sqrt[3]{2})$.

3.3 We use a similar method in this problem. When p is prime, ζ_p satisfies the irreducible Cyclotomic polynomial $x^{p-1} + x^{p-2} + \cdots + x + 1$ so we obtain towers

$\mathbb{Q} \subset \mathbb{Q}(\zeta_5) \subset \mathbb{Q}(\zeta_5, \zeta_7)$ and $\mathbb{Q} \subset \mathbb{Q}(\zeta_7) \subset \mathbb{Q}(\zeta_5, \zeta_7)$.

The bottom two extensions have degrees 4 and 6 respectively. If $\zeta_5 \in \mathbb{Q}(\zeta_7)$, then $[\mathbb{Q}(\zeta_5, \zeta_7) : \mathbb{Q}(\zeta_5)] = 1$, but then the total degree would be $[\mathbb{Q}(\zeta_5, \zeta_7) : \mathbb{Q}] = [\mathbb{Q}(\zeta_5, \zeta_7) : \mathbb{Q}(\zeta_5)][\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$. Since 4 is not divisible by 6, we have a contradiction.

3.7 (a) Again, we use the same approach. $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ (using irreducible polynomial $x^2 + 1$) and we compute $[\mathbb{Q}(\sqrt[4]{-2}) : \mathbb{Q}] = 4$ (using irreducible polynomial $x^4 + 2$, which is irreducible by the Eisenstein criterion). If $i \in \mathbb{Q}(\sqrt[4]{-2})$, then the total degree $[\mathbb{Q}(\sqrt[4]{-2}, i) : \mathbb{Q}]$ would also equal 4 and so $\sqrt[4]{-2}$ would have degree 2 over $\mathbb{Q}(i)$. However, factoring $x^4 + 2$ over $\mathbb{Q}(\sqrt[4]{-2})$, we get $x^4 + 2 = (x^2 + \sqrt{-2})(x^2 - \sqrt{-2}) = (x - \sqrt[4]{-2})(x + \sqrt[4]{-2})(x^2 + \sqrt{-2})$, which equals $(x - \sqrt[4]{-2})(x + \sqrt[4]{-2})(x - i\sqrt[4]{-2})(x + i\sqrt[4]{-2})$ in a splitting field. There is no way to combine these linear factors into quadratics with coefficients over $\mathbb{Q}(i)$ so i is not in $\mathbb{Q}(\sqrt[4]{-2})$.

(b) The irreducible polynomial for $\alpha = \sqrt[3]{5}$ is $x^3 - 5$, which has no rational root by the rational root test or is irreducible by the Eisenstein criterion. The irreducible polynomial for $\beta = \sqrt[3]{2}$ is $x^3 - 2$ analogously. Thus α and β both have degree 3 over $\mathbb{Q}$, but if we let $K = \mathbb{Q}(\alpha, \beta)$, we see that $[K : \mathbb{Q}] > 3$ since $x^3 - 5$ still has no root over $\mathbb{Q}(\alpha)$. Hence α is not in the field $\mathbb{Q}(\beta)$.

4.2 (a) Let $\alpha = \sqrt{3}+\sqrt{5}$. Then over $\mathbb{Q}$, we take the fourth power of α and compare it with the square of α and obtain a linear relation among $\alpha^4 = 32\sqrt{15}+124$, $\alpha^2 = 2\sqrt{15}+8$, and 1. Thus α is a root of $f = x^4 - 16x^2 + 4$. By the rational root test, f has no rational roots, and we must write down the product of two general monic quadratics $(x^2+ax+b)(x^2+cx+d)$ and conclude that there are no rational solutions to $(a+c)x^3 = 0x^3$, $(b+d+ac)x^2 = -16x^2$, $(ad+bc)x = 0x$, and $bd = 4$.

Thus f is the irreducible polynomial for α over $\mathbb{Q}$.

(b) Recall, that we have previously proven that $\sqrt{5} \in \mathbb{Q}(\alpha)$. In particular, $\sqrt{5} = c_1\alpha^3 + c_2\alpha$ for some $c_1, c_2 \in \mathbb{Q}$. So consider the tower $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\alpha)$. Since we just proved that the total degree is degree 4 and $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$, then $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{5}] = 2$.

In a splitting field, $f = x^4 - 16x^2 + 4$ factors as $(x-\sqrt{3}-\sqrt{5})(x-\sqrt{3}+\sqrt{5})(x+\sqrt{3}-\sqrt{5})(x+\sqrt{3}+\sqrt{5})$. Thus multiplying together conjugates, we see α is a root of the quadratic $(x-\sqrt{5}-\sqrt{3})(x-\sqrt{5}+\sqrt{3}) = (x-\sqrt{5})^2 - 3 = x^2 - 2\sqrt{5}x + 2$, which is irreducible in $\mathbb{Q}(\sqrt{5})[x]$. Note that we see that α satisfies $(\alpha - \sqrt{5}) = \sqrt{3}$ so $(\alpha-\sqrt{5})^2 - 3 = 0$ can also be seen directly.

(d) Finally, $\alpha^2 = 2\sqrt{15}+8$, so in $\mathbb{Q}(\sqrt{15})$, we have the irreducible polynomial $x^2 - (2\sqrt{15}+8)$.

Math 5286H: Fundamental Structures of Algebra II

HW 4 Solutions, (April 4th, 2012)

Problems from Chapter 15 of Artin's Algebra:

5.1 We start with the fact that $(\cos 30°, \sin 30°) = (\sqrt{3}/2, 1/2)$ is constructible. Thus suppose we were given the initial points $P = (0,0)$ and $Q = (1,0)$, and constructed $R = (\cos 30°, \sin 30°)$. We wish to construct the point $S = (\cos 15°, \sin 15°)$ by bisecting the angle.

Answer: Choose a radius r and construct the circles of radius r around points Q and R. We have points of intersection given by the equations

$$(x - \sqrt{3}/2)^2 + (y - 1/2)^2 = r = (x-1)^2 + y^2.$$

For example, if we let $r = 1$ then $P = (0,0)$ and $T = (1 + \sqrt{3}/2, 1/2)$ are the two points of intersection. We then construct the line from P to T and intersect it with the circle of radius 1 around $P = (0,0)$. We thus need to solve $x^2 + y^2 = 1$ where $y/x = (1/2)/(1 + \sqrt{3}/2) = 2 - \sqrt{3}$. Hence $(1 + (2-\sqrt{3})^2)x^2 = 1$ and the positive solution $x = \frac{1}{\sqrt{8-4\sqrt{3}}}$. We can rewrite the denominator as $\sqrt{2}(\sqrt{4-2\sqrt{3}}) = \sqrt{2}(\sqrt{3}-1) = \sqrt{6} - \sqrt{2}$. Thus we conclude that $x = \frac{1}{\sqrt{6}-\sqrt{2}} = \frac{\sqrt{6}+\sqrt{2}}{4}$ is cosine of 15 degrees.

Remark: See problem 16.6.3. The solution to this problem implies that many times a nested radical of the form $\sqrt{a + \sqrt{b}}$ can be rewritten as $\sqrt{c} + \sqrt{d}$.

Answer 2: We also have the half-angle formula $\cos(\frac{\theta}{2}) = \sqrt{\frac{1}{2} + \frac{\cos(\theta)}{2}}$. Applying this for $\theta = 30°$, we obtain $\cos 15° = \sqrt{\frac{1}{2} + \frac{\sqrt{3}}{4}} = \frac{\sqrt{6}+\sqrt{2}}{4}$.

Remark: Note that by a slight generalization of the above bisection construction, you can actually prove the half-angle formula for general θ.

6.3 Recall Proposition 13.2.2 which stated that the only units in the ring of integers in an imaginary quadratic number field $\mathbb{Q}(\sqrt{d})$ are ± 1 unless $d = -1$ or -3. (This was proven by noting that the norm of a unit would be one and $N(\alpha) = N(a + b\sqrt{d}) \neq 1$ if $b \neq 0$ unless $d = -1$ or -3.) Considering the problem at hand, if ζ_n is a primitive nth root of unity, note that $(\zeta_n)(\zeta_n^{n-1}) = 1$ which implies ζ_n would be a unit. Furthermore, ζ_n is an algebraic integer since it is a root of the integer polynomial $x^n - 1$. Thus $\mathbb{Q}(\sqrt{-1})$,

containing $\zeta_4 = i$, and $\mathbb{Q}(\sqrt{-3})$, containing $\zeta_3 = \frac{-1-\sqrt{3}}{2}$ and $\zeta_6 = \frac{1-\sqrt{3}}{2}$, are the only imaginary quadratic number fields containing a primitive nth root of unity (other than the trivial cases of $n = 1$ or 2).

Remark: Also note that a quadratic number field $\mathbb{Q}(\sqrt{d})$ has degree two over $\mathbb{Q}$ since we are adjoining a root fo the irreducible polynomial $x^2 - d$. If $\mathbb{Q}(\sqrt{d})$ contains ζ_n, a primitive nth root of unity (other than ± 1), then $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\zeta_n, \sqrt{d})$ and so ζ_n must be degree two over $\mathbb{Q}$. We observe that ζ_3 satisfies $x^2 + x + 1$, ζ_4 satisfies $x^2 + 1$ and ζ_6 is a root of $x^2 - x + 1$. We will see next week that for $n > 6$, ζ_n has an irreducible polynomial (called the nth cyclotomic polynomial) of degree > 2, even when n is composite.

7.4 By Theorem 15.7.3 (b), the set of irreducible polynomials over $\mathbb{F}_p$ with degree dividing 3 coincide with the set of irreducible factors of $x^{p^3} - x$ in $\mathbb{F}_p[x]$.

Letting $p = 3$, we factor $x^{27} - x$ into irreducibles, noting that there are three linear factors $x(x-1)(x-2)$, and all other factors must be the set of irreducible polynomials over $\mathbb{F}_3$ of degree 3. Since we are factoring a degree 24 polynomial into irreducible cubics, we conclude that there are eight irreducible cubics over $\mathbb{F}_3$.

By similar logic, we obtain 40 irreducible cubics over $\mathbb{F}_5$.

7.5 As described in Problem 7.4, over $\mathbb{F}_3$, the polynomial $x^9 - x$ factors as $x(x-1)(x-2)P_1P_2P_3$ where P_1, P_2, and P_3 are the three irreducible quadratics over $\mathbb{F}_3$. We can thus do the synthetic division by $x(x-1)(x+1)$ and then peel off an irreducible quadratic one at a time, or list the nine monic quadratics $\{x^2 + ax + b : a, b \in \{-1, 0, 1\}\}$, and cross out the ones which contain a root in $\mathbb{F}_3$.
Either way, we obtain the answer of $x^9 - x = x(x+1)(x-1)(x^2+1)(x^2+x-1)(x^2-x-1)$. We similarly factor

$$x^{27} - x = x(x+1)(x-1)(x^3-x+1)(x^3-x-1)(x^3+x^2-1)(x^3+x^2+x-1)(x^3+x^2-x+1)(x^3-x^2+1)(x^3-x^2+x+1)(x^3-x^2-x-1).$$

7.7 This is actually a generalization of Wilson's Theorem (Problem 1.8 (b) from Chapter 3). Notice that $|K| = q = p^k$ for some prime p, and $|K^\times| = q - 1$. Since $K^\times$ is cyclic, let α be a generator. Then the product, β, of all nonzero elements of K is the same as multiplying together $\alpha\alpha^2\alpha^3 \cdots \alpha^{q-2} = \alpha^{1+2+\cdots+(q-2)} = \alpha^{(q-1)q/2}$. Hence $\beta = \alpha^{(q-1)q/2}$. Notice that $\beta^2 = (\alpha^{q-1})^q = 1^q = 1$ so β is a square root of unity.

We now have two cases depending on whether or not char $K = 2$. If char $K \neq 2$, then q is odd and we can write it as $q = 2r + 1$. If we reduce $(q-1)q/2$ modulo $(q-1)$, we get $(q-1)r + (q-1)/2 \equiv (q-1)/2 \mod (q-1)$. Thus $\beta = \alpha^{(q-1)/2} \neq 1$ and so $\beta = -1$.

On the other hand, if char $K = 2$, then $\beta^2 = 1$ implies $\beta = 1 \equiv -1$ in this case. Thus no matter what the characteristic is, we obtain the desired formula.

Answer 2: We also can use the fact that each $x \in \mathbb{F}_q^\times$ besides $x = 1$ and $x = -1$ have a unique inverse (note that -1 is distinct from 1 if and only if $q \neq 2^r$). Thus pairing those off, we are left with $-1 \cdot 1 = -1$. Note that this proof is implicitly using the fact that $\mathbb{F}_q^\times$ is cyclic to imply that every $x \in \mathbb{F}_q^\times$ can be written

as α^i for $i \in \{0, 1, 2, \ldots, q-2\}$, and thus $x^{-1} = \alpha^{q-1-i}$ which is distinct from α^i if $i \neq 0$ or $\frac{q-1}{2}$ when q is odd. If cyclicity of $\mathbb{F}_q^\times$ is not mentioned, then another reason why most elements have a unique inverse for a general finite field must be explained.

7.8 Let $f = x^3+x+1$ and $g = x^3+x^2+1$, which are both irreducible over $\mathbb{F}_2$. Let $K = \mathbb{F}_2[x]/(x^3+x+1) = \mathbb{F}_2(\alpha)$ and $L = \mathbb{F}_2[x]/(x^3+x^2+1) = \mathbb{F}_2(\beta)$. Since K and L both are degree 3 over $\mathbb{F}_2$, they are isomorphic fields of order 8.

To see this isomorphism explicitly, we note that in K, α, α^2 and $\alpha^2+\alpha$ are the three roots of $f(x)$. (We see this by plugging in α^2 and $\alpha^2+\alpha$ and using the fact that $\alpha^3+\alpha+1 \equiv 0$.) We also can compute that in L, $\beta+1$, β^2+1, and $\beta^2+\beta$ are the three roots of $f(x)$ (using that $\beta^3+\beta^2+1 \equiv 0$.)

Since $f(x)$ is irreducible in $\mathbb{F}_2$, by Proposition 15.2.8, there exists an isomorphism from α to each of $\beta+1$, β^2+1, and $\beta^2+\beta$. Thus there exists three such isomorphisms $\{\sigma_1, \sigma_2, \sigma_3\}$ from K to L.

$$\sigma_1(\alpha) = \beta+1, \qquad \sigma_1(\alpha^2) = (\beta+1)^2 = \beta^2+1, \qquad \sigma_1(\alpha^2+\alpha) = (\beta^2+1)+(\beta+1) = \beta^2+\beta.$$

$$\sigma_2(\alpha) = \beta^2+1, \qquad \sigma_2(\alpha^2) = (\beta^2+1)^2 \equiv \beta^2+\beta, \qquad \sigma_2(\alpha^2+\alpha) = (\beta^2+\beta)+(\beta^2+1) = \beta+1.$$

$$\sigma_3(\alpha) = \beta^2+\beta, \qquad \sigma_3(\alpha^2) = (\beta^2+\beta)^2 \equiv \beta+1, \qquad \sigma_3(\alpha^2+\alpha) = (\beta+1)+(\beta^2+\beta) = \beta^2+1.$$

8.1 Let K be a finite extension of finite field F. Then K is a finite-dimensional vector space over a finite field, and thus K is also a finite field. Thus $|K| = q = p^r$ for some prime power, and by Theorem 15.7.3 (c), $K^\times$ is a cyclic group of order $(q-1)$. Let α be a generator for $K^\times$. We claim that $K = F(\alpha)$ in this case.

To prove this, we note that $K = \{0\} \cup K^\times = \{0\} \cup \{\alpha, \alpha^2, \ldots, \alpha^{q-2}\} \subset F(\alpha)$. Since $|K| = |F(\alpha)|$ as sets, we conclude the desired equality.

Remark: While you did not need to show it, for an *infinite* and *perfect* field the proof of the Primitive Element Theorem given in Section 15.8 will work with little adaptation. By induction, we consider the case $K = F(\alpha, \beta)$, a finite extension of F. For all but finitely many $c \in F$, we see that $\gamma = \beta + c\alpha$ is a primitive element by essentially using Lemma 15.8.2.

Note that for the finite field case, this argument would not quite show that there still existed a $c \in F$ to choose, but one could more carefully count the number of "bad" values for c in the second paragraph. However, going back to the infinite perfect field case, we again know the roots of an irreducible polynomial are distinct in an extension, since in a perfect field, irreducible implies separable (see class notes).

Problems from Chapter 16 of Artin's Algebra:

1.3 (a) There are several different common proofs in the literature. Wikipedia actually presents a decent number of them. See "Derivation of the Identities" near the bottom of the page

http://en.wikipedia.org/wiki/Newton for some examples. More on symmetric functions is also available at http://ocw.mit.edu/courses/mathematics/18-312-algebraic-combinatorics-spring-2009/readings-and-lecture-notes/MIT18_312S09_lec18_Symm.pdf

b) The symmetric polynomials $w_1, \ldots, w_k$ generate the ring of symmetric functions in $R[x_1, \ldots, x_n]$ for any R where the numbers $\{1, 2, \ldots, n\}$ have inverses. To see this, we use the fact that $s_1, \ldots, s_k$ generate the symmetric functions in $R[x_1, \ldots, x_n]$ by Theorem 16.1.6 and if 1 through n are invertible, we can write $s_k = \pm\frac{1}{k}(w_k - s_1 w_{k-1} + s_2 w_{k-2} + \cdots \pm s_{k-1} w_1)$. Thus by induction, we can write $s_1 = w_1$, $s_2 = \frac{1}{2}(w_2 - s_1 w_1), \ldots$ and using w_1 through w_n we can generate all of the s_i's, and hence the ring of symmetric functions.

Remark: So for example, if $R = \mathbb{Q}$, the w_i's do generate, if $R = \mathbb{Z}$ or $\mathbb{F}_p$ for $p \leq n$, then the w_i's do not.

2.2 (a) Let $D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$ where α_1, α_2, and α_3 are the three roots of a real cubic $f(x)$.

Then $D = 0$ if and only if $f(x)$ has repeated roots. In this case, in its splitting field, $f(x) = (x-\alpha_1)^2(x-\alpha_3)$. Since $f(x)$ has real coefficients, we can take the complex conjugate, $f(x) = \overline{f(x)} = (x - \overline{\alpha_1})^2(x - \overline{\alpha_3})$ and we get the same roots. Since the root multiplicities must coincide, we see that $\overline{\alpha_1} = \alpha_1$ and $\overline{\alpha_3} = \alpha_3$, so all three of $f(x)$'s roots are real in this case.

Now assume $D \neq 0$ so that $f(x)$ has distinct roots. We again need complex conjugation to induce a permutation on the three roots. However, since complex conjugation has order 2 but there are three roots, it must fix one of the roots or all three of the roots. Note that complex conjugation also acts on $\sqrt{D} = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$.

If complex conjugation fixes all three roots, then $\overline{\sqrt{D}} = \sqrt{D}$ and we conclude that $\sqrt{D}$ is real, hence $D > 0$. If complex conjugation fixes exactly one root, e.g. α_3, then $\overline{\sqrt{D}} = (\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3) = -\sqrt{D}$ and we conclude that $\sqrt{D}$ is imaginary, hence $D < 0$.

(b) Analogously, a real quartic polynomial $g(x)$ has 0, 2, or 4 real roots since complex roots come in conjugate pairs again. We assume $\sqrt{D} = \prod_{1 \leq i < j \leq 4}(\alpha_i - \alpha_j)$ is real since $D > 0$.

We consider the three possible cases: (i) if $g(x)$ has no real roots, then there are two pairs of complex conjugates, e.g. $\overline{\alpha_1} = \alpha_2$ and $\overline{\alpha_3} = \alpha_4$ so $g(x) = \overline{g(x)}$ induces the symmetry $\overline{D} = (12)(34)D = (-1)^2 D = D$, which is consistent with $D \in \mathbb{R}$.

(ii) if $g(x)$ has two real roots, then there is one pair of complex conjugates, e.g. $\overline{\alpha_1} = \alpha_2$ and $\overline{\alpha_3} = \alpha_3$, $\overline{\alpha_4} = \alpha_4$ so $g(x) = \overline{g(x)}$ induces the symmetry $\overline{D} = (12)D = -D$, which is inconsistent.

(iii) if $g(x)$ has four real roots, then $\overline{\alpha_1} = \alpha_2$ and $\overline{\alpha_3} = \alpha_3$, $\overline{\alpha_4} = \alpha_4$ so $g(x) = \overline{g(x)}$ induces the symmetry $\overline{D} = D$, which is again consistent.

We thus conclude from $D > 0$ that $f(x)$ has 0 or 4 real roots.

3.1 Let K/F be a splitting field for $f(x)$ over F, such that $f(x)$ has degree n. Let α_1 be a root of $f(x)$. Then $[F(\alpha_1) : F] \leq n$ We now will compute $[K : F(\alpha_1)] \leq (n-1)!$ shortly, thus concluding that

$[K:F] = [K:F(\alpha_1)][F(\alpha_1):F] \leq (n-1)! \cdot n = n!$.

Note that over $F(\alpha_1)$, then $f(x)$ factors as $(x-\alpha_1)g(x)$ where the degree of $g(x)$ is $(n-1)$. Thus we build a tower and conclude

$$\begin{aligned}[K:F] &= [K:F(\alpha_{n-1},\alpha_{n-2},\ldots,\alpha_1)]\,[F(\alpha_{n-1},\alpha_{n-2},\ldots,\alpha_1):F(\alpha_{n-2},\ldots,\alpha_1)]\cdots[F(\alpha_2,\alpha_1):F(\alpha_1)]\,[F(\alpha_1):F] \\ &\leq 1\cdot 2\cdots(n-1)n.\end{aligned}$$

We now prove that [K:F] divides n! by strong induction: The base case $n=1$ follows easily. Now assume for $1 \leq k \leq n-1$ that a polynomial of degree k has a splitting field of degree m, which divides $k!$.

We have two cases. First let $f(x)$ be a polynomial in $F[x]$ of degree n that is irreducible. Then letting α be a root of $f(x)$, we see that $f(x) = (x-\alpha)g(x)$ where $g(x) \in F(\alpha)[x]$ is of degree $n-1$. By induction, the splitting field K for $g(x)$ has degree dividing $(n-1)!$ and so $[K:F] = [K:F(\alpha)][F(\alpha):F]$ divides $n!$.

In the second case, suppose that $f(x)$ reduces as $g(x) * h(x)$ in $F[x]$. Here, $g(x)$ and $h(x)$ could also be reducible but at least of lower degree, say degrees m and $(n-m)$. Let K_1 be the splitting field for $g(x)$ and K_2 be the splitting field for $h(x)$. By strong induction, we see that $[K_1:F]$ divides $m!$ and $[K_2:F]$ divides $(n-m)!$.

The splitting field K for $f(x)$ is a field extension of both K_1 and K_2 so we have $[K:F]$ divides $[K_1:F][K_2:F]$, and hence divides $m!(n-m)!$. Finally, we use the fact that binomial coefficients $\binom{n}{m}$ are integers to conclude that $m!(n-m)!$ divides $n!$ and hence $[K:F]$ divides $n!$ in the case too.

Remark: Several students used results such as Theorems 16.6.4 and 16.6.6 to state that K/F is Galois since K is a splitting field for $f(x) \in F[x]$ and that $Gal(K/F)$ is a subgroup of S_n, where n is the degree of $f(x)$. Thus $[K:F] = |Gal(K/F)|$ divides $|S_n| = n!$ by Lagrange's Theorem. The problem with this argument is that Artin only proves Theorem 16.6.4 in Charatersitic zero, i.e. when the Primitive Element Theorem applies. However, the above argument will work in characteristic p also.

3.2 (b) x^4-1 splits as $(x^2+1)(x^2-1) = (x-i)(x+i)(x+1)(x-1)$ and so the splitting field is $\mathbb{Q}(i)$ which has degree two over $\mathbb{Q}$ since i is a root of irreducible x^2+1.

(c) x^4+1 splits as $(x^2+i)(x^2-i) = (x-\frac{\sqrt{2}}{2}(1+i))(x-\frac{\sqrt{2}}{2}(-1-i))(x-\frac{\sqrt{2}}{2}(1-i))(x-\frac{\sqrt{2}}{2}(-1+i))$.

Thus, the splitting field for x^4+1 is $K = \mathbb{Q}(\sqrt{2},\sqrt{2}i) = \mathbb{Q}(\sqrt{2},i) = \mathbb{Q}(\sqrt{2}(1+i))$. Since $K = \mathbb{Q}(\sqrt{2},i) \supset \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i) \supset \mathbb{Q}$, we can obtain K as a combination of two quadratic extensions, and hence $[K:\mathbb{Q}] = 4$. (We also can see this since one of the roots of x^4+1 is also a primitive element for $K/\mathbb{Q}$.)

4.1 (a) Any automorphism σ of a field K containing $\mathbb{Q}$ must fix $\mathbb{Q}$ since $\sigma(1) = 1$. Thus, we are really asked to compute $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ and $Gal(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})$ where $\omega = e^{2\pi/3}$.

As in class, $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$ and $Gal(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}) = S_3 = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ where $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega$ and $\tau(\omega) = \overline{\omega}$. Notice σ has order 3 and τ has order 2.

(b) Let K_1 be the splitting field for $x^2 - 2x - 1$ over $\mathbb{Q}$ and K_2 be the splitting field for $x^2 - 2x - 7$. Then since these are both quadratic polynomials, $K_1 = \mathbb{Q}(\sqrt{a})$ and $K_2 = \mathbb{Q}(\sqrt{b})$ for some non-squares $a, b \in \mathbb{Q}$. Thus $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$. However, looking at closer at the roots of these two equations, we see that we can choose $a = b = 2$ for these two equations, and thus $K = \mathbb{Q}(\sqrt{2})$ and so there are only two automorphisms of K, $\{1, \tau\}$ where $\tau : \sqrt{2} \to -\sqrt{2}$.

6.2 Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Since $\sqrt{2} \notin \mathbb{Q}$, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, and $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$, we conclude that K can be obtained by three quadratic extensions. (Note: if we did have such inclusions, we would have an equality such as $\sqrt{5} = a\sqrt{2} + b\sqrt{3}$ for some rational numbers a and b and by squaring both sides, we would include that a rational 5 was equal to an irrational, $2a^2 + 3b^2 + 2ab\sqrt{6}$.) Thus $[K : \mathbb{Q}] = 2^3 = 8$.

Since K yields $\mathbb{Q}$-automorphisms $\sigma_1 : \sqrt{2} \to -\sqrt{2}$, $\sigma_2 : \sqrt{3} \to -\sqrt{3}$, and $\sigma_3 : \sqrt{5} \to -\sqrt{5}$, we see that $Gal(K/\mathbb{Q}) = C_2 \times C_2 \times C_2$, which has order 8. (We know there cannot be more automorphisms, since $|Gal(K/\mathbb{Q})| > [K : \mathbb{Q}]$ impossible.) Thus $[K : \mathbb{Q}] = |Gal(K/\mathbb{Q})|$, and we conclude that $K/\mathbb{Q}$ is Galois.

6.3 Let $K \supset L \supset F$ be a chain of extension fields of degree 2. Then $L = F(\sqrt{a})$ for some $a \in F$ such that $x^2 - a$ is irreducible$/F$. Since K is a quadratic extension over L, then $K = F(\sqrt{a}, \sqrt{\beta})$ where $\beta \in F(\sqrt{a})$ but $x^2 - \beta$ is irreducible$/L$.

By the Primitive Element Theorem, $K = F(\gamma)$ where $\gamma = \sqrt{a} - c\sqrt{\beta}$ for some $c \in F$.

We thus conclude that K is generated by an element γ that is either a sum involving a nested radical, $\sqrt{a} + \sqrt{b + d\sqrt{a}}$, (with $a, b, d \in F$) or the sum of two square-roots, $\sqrt{a} + \sqrt{b}$, (if $\beta = b \; in F$). Furthermore, in the first case, we note that $\gamma' = \sqrt{b + d\sqrt{a}}$ is also a primitive element since $\sqrt{a} = \frac{(\gamma')^2 - b}{d}$, and thus $K = F(\sqrt{a}, \sqrt{\beta}) = F(\sqrt{\beta})$.

So pick $\gamma = \sqrt{a} + \sqrt{b}$ (resp. $\sqrt{b + d\sqrt{a}}$), and observe that γ^4 and $\gamma^2 \in F(\sqrt{ab})$ (resp. $F(\sqrt{a})$). Thus there is a polynomial $f(x)$ in $F[x]$ with basis x^4, x^2, and 1 so that $f(\gamma) = 0$. Furthermore, $f(x)$ irreducible in F since it factors into quadratics with coefficients in a quadratic extension of F.

Remark: One can also compute the Galois group of K/F and conclude that it must be C_4 or $C_2 \times C_2$, and consider the intermediate fields in these two cases to describe an explicit form for γ, the primitive element generating K over F.

Math 5286H: Fundamental Structures of Algebra II

HW 5 Solutions, (April 27th, 2012)

Problems from Chapter 16 of Artin's Algebra:

9.3 As discussed in class and in the book (Examples 16.9.2 (c)), if $\alpha = \sqrt{4+\sqrt{7}}$, then letting K be the splitting field of α's irreducible polynomial, we have that $Gal(K/\mathbb{Q}) \cong V_4 = C_2 \times C_2$. Consequently, K has degree 4 over $\mathbb{Q}$, and $K = \mathbb{Q}(\alpha)$. K also contains three different quadratic extensions (over $\mathbb{Q}$) as subfields. Since a quadratic extension over $\mathbb{Q}$ looks like $\mathbb{Q}(\sqrt{a})$ where a is a square-free integer, and two quadratic extensions, $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$, are different if only if $a \neq b$, consider $\mathbb{Q}(\sqrt{a}+\sqrt{b})$, which would be a degree 4 extension of $\mathbb{Q}$ contained inside K. We conclude that $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{a}+\sqrt{b})$, where a' and b' are rational square multiples of a and b, and hence $\alpha = \sqrt{a'} + \sqrt{b'}$ for some rational a' and b'.

Answer 2: We can also find a and b explicitly by letting $\alpha' = \sqrt{4-\sqrt{7}}$ and noting that $\pm\alpha$ and $\pm\alpha' \in K$, as these are the four roots of α's irreducible polynomial. Consequently, $\sqrt{\alpha^2 \pm 2\alpha\alpha' + \alpha'^2} = \alpha \pm \alpha' \in K$, thus $\sqrt{(4+\sqrt{7}) \pm 2\sqrt{16-7} + (4-\sqrt{7})} = \sqrt{8 \pm 6}$. Thus $\sqrt{2}$ and $\sqrt{14}$ are in K.

Trying $(\sqrt{2}+\sqrt{14})^2 = 16 + 2\sqrt{28}$, we see this equals 4α, thus $\alpha = \sqrt{\frac{1}{2}} + \sqrt{\frac{7}{2}}$.

In fact $\frac{\sqrt{2}+\sqrt{14}}{2} = \frac{\alpha+\alpha'}{2} + \frac{\alpha-\alpha'}{2} = \alpha$, so it was clear that this particular linear combination would work.

9.6 Using the discrimiant formula $D = 256s^2(r^2-s)$ for a quartic of the form $x^4 - 2rx^2 + (r^2-s)$ from class, letting $r = 0$ and $s = -1$ we get $D = 256$ and so $\sqrt{D} \in \mathbb{Q}$. One could also compute the roots of x^4+1 explicitly and compute $D = \prod_{1 \leq i < j \leq 4}(\alpha_i - \alpha_j)^2$.

In particular, x^4+1 is the irreducible polynomial for ζ_8, a primitive 8th root of unity, and $x^4+1 = (x-\zeta_8)(x-\zeta_8^3)(x-\zeta_8^5)(x-\zeta_8^4)$. Thus the Galois group could be A_4 or V_4 by Proposition 16.9.5. By looking at resolvent cubics or otherwise, we can find that the Galois group is in fact $V_4 \cong C_2 \times C_2$. For example, since we already observed that x^4+1 is the irreducible polynomial for ζ_8, that means it's splitting field is $\mathbb{Q}(\zeta_8)$, which has Galois group $(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\} \cong V_4$ over $\mathbb{Q}$, agreeing with above.

9.8 Let $\alpha = \sqrt{r+\sqrt{t}}$ and $\alpha' = \sqrt{r-\sqrt{t}}$. If α can also be written as $\sqrt{a}+\sqrt{b}$, then $\mathbb{Q}(\alpha)$ has three subfields, $\mathbb{Q}(\sqrt{a})$, $\mathbb{Q}(\sqrt{b})$, and $\mathbb{Q}(\sqrt{ab})$ if a and b are not squares. (Note that these fields might coincide if a or b is a square.)

Since $\alpha\alpha'$, $\alpha+\alpha'$ and $\alpha-\alpha'$ are the only elements possibly fixed by a transposition, if $\alpha=\sqrt{a}+\sqrt{b}$, then $\alpha\alpha'$, $\alpha+\alpha'$ or $\alpha-\alpha'$ must generate $\mathbb{Q}(\sqrt{a})$, $\mathbb{Q}(\sqrt{b})$, and $\mathbb{Q}(\sqrt{ab})$. We thus restrict our attention to the cases of $\alpha\pm\alpha'$.

Because of the identity $\alpha=\frac{\alpha+\alpha'}{2}+\frac{\alpha-\alpha'}{2}$, we simply check whether $\alpha\pm\alpha'=\sqrt{\alpha^2\pm2\alpha\alpha'+\alpha'^2}$ can both be written as non-nested square-roots, as was the case in Problem 16.9.3.

(a) Let $\alpha=\sqrt{2+\sqrt{11}}$. Then $\alpha^2\pm2\alpha\alpha'+\alpha'^2=4\pm2\sqrt{-7}$, so we cannot write α as a sum of two square-roots.

(b) Let $\alpha=\sqrt{10+5\sqrt{2}}$. Then $\alpha^2\pm2\alpha\alpha'+\alpha'^2=20\pm2\sqrt{50}$, so we cannot write α as a sum of two square-roots.

(c) Let $\alpha=\sqrt{11+6\sqrt{2}}$. Then $\alpha^2\pm2\alpha\alpha'+\alpha'^2=22\pm2\sqrt{121-72}=22\pm14$, so we can write α as a sum of two square-roots. Namely, $\alpha=\frac{\sqrt{36}+\sqrt{8}}{2}=3+\sqrt{2}$.

(d) Let $\alpha=\sqrt{6+\sqrt{11}}$. Then $\alpha^2\pm2\alpha\alpha'+\alpha'^2=12\pm2\sqrt{36-11}=12\pm10$, so we can write α as a sum of two square-roots. Namely, $\alpha=\frac{\sqrt{22}+\sqrt{2}}{2}=\sqrt{\frac{11}{2}}+\sqrt{\frac{1}{2}}$.

(e) Let $\alpha=\sqrt{11+\sqrt{6}}$. Then $\alpha^2\pm2\alpha\alpha'+\alpha'^2=22\pm2\sqrt{115}$, so we cannot write α as a sum of two square-roots.

9.11 (a) Since α is real but $i\alpha$ is not, we see that $i\alpha\notin\mathbb{Q}(\alpha)$ so the splitting field K for x^4+2 is $\mathbb{Q}(\alpha,i\alpha)$ which has degree 8 over $\mathbb{Q}$ since $i\alpha$ is a root of irreducible $x^2+\alpha^2=x^2+\sqrt{2}$ over $\mathbb{Q}(\alpha)$.

Since D_4 is the only order eight transitive subgroup of S_4, we conclude that $G=Gal(K/F)=D_4$.

The two generators of G are σ of order 4, which sends α to $i\alpha$ (and leaves i fixed), and τ of order 2, which sends i to $-i$ (and leaves α fixed).

Thus $H=Gal(K/F(i))$ is the subgroup of automorphisms that fix $F(i)$, namely $\langle\sigma\rangle\cong C_4$.

(b) See part (a).

(c) D_4 has proper subgroups $\langle\sigma\rangle\cong C_4$; $\langle\sigma^2,\tau\rangle$ or $\langle\sigma^2,\sigma\tau\rangle\cong C_2\times C_2$; and $\langle\tau\rangle$, $\langle\sigma\tau\rangle$, $\langle\sigma^2\tau\rangle$, $\langle\sigma^3\tau\rangle$, or $\langle\sigma^2\rangle\cong C_2$. Looking at the fixed fields of these subgroups, the intermediate fields, in respective order, are

$$F(i);\quad F(\sqrt{2}),\ F(i\sqrt{2});\quad F(\sqrt[4]{2}),\ F(\sqrt[4]{2}+i\sqrt[4]{2}),\ F(i\sqrt[4]{2}),\ F(\sqrt[4]{2}-i\sqrt[4]{2}),\quad \text{and}\quad F(\sqrt{2},i).$$

10.3 Let $\zeta=\zeta_7$. The Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ is $\langle\sigma\rangle\cong C_6$, where $\sigma(\zeta)=\zeta^3$ since 3 is a primitive root modulo 7 ($3^1\equiv3, 3^2\equiv2$, $3^3\equiv6$, $3^4\equiv4$, $3^5\equiv5$, and $3^6\equiv1$).

(a) Since $\sigma(\zeta+\zeta^5)=\zeta^3+\zeta$, $\sigma^2(\zeta+\zeta^5)=\zeta^2+\zeta^3$, and $\sigma^3(\zeta+\zeta^5)=\zeta^6+\zeta^2$, we see that $\zeta+\zeta^5$ is not fixed by any element of $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ except for the identity. Thus $\zeta+\zeta^5$ has degree 6 over $\mathbb{Q}$.

(b) Since $\sigma(\zeta^3+\zeta^4)=\zeta^2+\zeta^5$, $\sigma^2(\zeta^3+\zeta^4)=\zeta^6+\zeta$, and $\sigma^3(\zeta^3+\zeta^4)=\zeta^4+\zeta^3$, we see that $\zeta^3+\zeta^4$ is fixed by the subgroup $H=\{1,\sigma^3\}$ and so by looking at the index of H in $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$, we see that $\zeta^3+\zeta^4$ has degree 3 over $\mathbb{Q}$.

(c) Since $\sigma(\zeta^3+\zeta^5+\zeta^6)=\zeta^2+\zeta+\zeta^4$ and $\sigma^2(\zeta^3+\zeta^5+\zeta^6)=\zeta^6+\zeta^3+\zeta^5$, then $\zeta^3+\zeta^5+\zeta^6$ is fixed by the subgroup $H=\{1,\sigma^2,\sigma^4\}$ and so by looking at the index of H in $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$, we see that $\zeta^3+\zeta^5+\zeta6$ has degree 2 over $\mathbb{Q}$.

12.1 If K/F is a Galois extension of degree 10, then $G=Gal(K/F)$ has order 10. Since 10 is the product of two primes, by earlier results (e.g. Problem 7.2.17), we see that G contains an element σ of order 5. Thus G contains a subgroup $H=\langle\sigma\rangle$ of order 5 and index 2. Since all subgroups of index two must be normal, recall that the left and right cosets agree in this case, H is normal in G and so we have a solvalbe chain of subgroups $\{1\}\subset H\subset G$ where each extension is of prime degree.

By Problem 16.M.12, this implies that there is a chain of intermediate fields $F\subset L\subset K$ where K/L and L/F are both Galois, and of prime degree (5 and 2, respectively). Thus K/F is solvable.

Remark: By looking at the chain of groups further, we can explictly compute that there are two possible groups of order 10, namely C_{10} or D_5, but this is not needed for the problem.

12.3 Since G is the Galois group of an irreducible quintic, then G acts transitiviely on the five roots, and hence G is a subgroup of S_5 that contains a 5-cycle σ. If G also contains an element α of order 3, then α must be a 3-cycle, since $5<2\cdot 3$. By relabeling, we can assume that $\sigma=(12345)$ and $\alpha=(1ij)$. Thus G also contains $\alpha^{-1}=(1ji)$. Consequently, we may assume, up to conjugating by σ (i.e. cyclic relabeling), that $\alpha=(123)$ or (124). Assume that $\alpha=(123)$ so that α^{-1} and their cyclic conjugates are in G. Then $(243)(132)(234)=(124)$ and so once (123) is in G, so is (124). Similar logic shows that we can obtain 3-cycles of the form (123) and (132) once we have them of the form (124). Consequently, G contains all 3-cycles, and as we showed on Midterm 1, problem 2b, last semester, A_n is generated by 3-cycles.

Thus G is either A_5 or S_5.

Remark: One can also approach this problem by noting that G's order must be divisible by both 3 and 5 (hence 15) by Lagrange's Theorem, and we look as possible subgroups of S_5 with order 15, 30, 60, or 120. By Sylow Theorems, we can eliminate the possibilities of order 15 and 30 groups, thus concluding that $G=A_5$ or S_5.

12.5 Let K be a Galois extension of $\mathbb{Q}$ whose degree is a power of 2 and such that $K\subset\mathbb{R}$.

We wish to show that the elements of K can be constructed by ruler and compass. By Theorem 15.5.10, it suffices to show that there is chain of fields $\mathbb{Q}=F_0\subset F_1\subset F_2\subset\cdots\subset F_n=K\subset\mathbb{R}$ so that $[F_{i+1}:F_i]=2$ for each extension.

Let $G = Gal(K/\mathbb{Q})$, which has order $2^m = [K : \mathbb{Q}]$ since K is a Galois extension over $\mathbb{Q}$. We will prove the result by induction on m, noting that the base case $m = 1$ is clear.

Since G is a p-group for $p = 2$, by Proposition 7.3.1, the center $Z(G)$ of G is a non-trivial subgroup. Since the center is a normal subgroup of a group, we have two cases:

Case 1: $Z(G) = G$, in which case G is abelian and any subgroup of G is normal. By Corollary 7.7.3, G contains an element τ of order 2 and letting $H = \{1, \tau\}$, we see that G contains a normal subgroup G/H of index two, and thus

K contains a subfield $L = K^{G/H} \subset \mathbb{R}$ such that $[K : L] = 2$, $L/\mathbb{Q}$ is also Galois and $Gal(L/\mathbb{Q})$ is of order 2^{m-1}. Thus we could continue by induction, and obtain that there is a full of chain of quadratic extensions between $\mathbb{Q}$ and K, via L.

Case 2: If $Z(G)$ is a proper subgroup of G, then we have a normal subgroup H of order 2^ℓ and thus we have a chain $\mathbb{Q} \subset L \subset K \subset \mathbb{R}$, where $L = K^H$, $[L : \mathbb{Q}] = 2^{m-\ell}$, $[K : L] = 2^\ell$ and both of these extensions are Galois. Also, ℓ and $m - \ell$ are both positive and smaller than m. Thus by induction, we can complete each of these chains separately and splice them together.

Either way, we have an inductive way to get the desired chain.

12.7 To find a polynomial of degree 7 over $\mathbb{Q}$ whose Galois group is S_7, we use the following result:

Lemma: Let p be a prime. Then the symmetric group S_p is generated by a p-cycle and a transposition.

Proof: By relabeling elements, assume that the p-cycle is $\sigma = (123 \dots p)$ and the transposition is $\tau = (1, k+1)$. Notice that $\sigma\tau\sigma^{-1} = (2, k+2)$, and repeating this we get $\sigma^k\tau\sigma^{-k} = (k+1, 2k+1)$. Notice that $(1, k+1)(k+1, 2k+1)(1, k+1) = (1, 2k+1)$. Inductively, we obtain the transpositions

$\{(1, k+1), (1, 2k+1), (1, 3k+1), \dots, (1, mk+1), \dots\}$ for all m. Since p is prime, there exists m so that $mk + 1 \equiv 2 \mod p$ (i.e. pick $m = k^{-1} \mod p$). We similarly obtain $\{(12), (13), \dots, (1p)\}$ by picking multiples of $m = k^{-1} \mod p$. We then conjugate these elements by the p-cycle σ, as above, to obtain all other transpositions (ij) in S_p. Since we have showed earlier in the course that S_p is generated by transpositions, we are done.

Remark: This Lemma was actually problem 16.12.8

Thus, in the $p = 7$ case, we see it suffices to find an irreducible polynomial (hence the Galois group acts transitively and contains a 7-cycle) where the Galois group contains a transposition. Since complex conjugation is an order two automorphism that is a transposition, rather than a product of transpositions, when there are exactly two complex roots, it suffices to find an irreducible degree 7 polynomial with exactly five real roots.

Example: $(x^3 - 2)(x^2 - 4)(x^2 - 16) + 2 = x^7 - 20x^5 - 2x^4 + 64x^3 + 40x^2 - 126$ for instance. The portion $(x^3 - 2)(x^2 - 4)(x^2 - 16)$ clearly has five real roots, and adding two will not affect this. This polynomial

is also irreducible by the Eisenstein criterion. Thus we have found a polynomial with Galois group S_7.

Remark: Though the logic at the beginning will probably be similar, there will be many different examples answering this problem.

M.12 (Bonus)

Let f be an irreducible polynomial over F with splitting field K. Let $G = Gal(K/F)$. We wish to show that G is solvable, that is there exists a chain of subgroups $\{1\} = H_k \subset H_{k-1} \subset \cdots \subset\subset H_1 \subset H_0 = G$ such that H_{i+1} is normal in H_i and the quotient groups H_i/H_{i+1} are each cyclic, if and only if all roots α of f are solvable (Definition from Proposition 16.12.2). Note the minor notational correction from Artin.

First assume that the group G is indeed solvable. Then by the Main Theorem (Theorem 16.7.1), there exists a chain of intermediate fields $F = F_0 \subset F_1 \subset \cdots \subset F_{k-1} \subset F_k = K$ such that F_i is the fixed field K^{H_i}.

Since H_1 is normal in $H_0 = G$, we see that both K/F_1 and $F_1/F_0 = F_1/F$ are Galois extensions. In particular, $Gal(K/F_1) = H_1$ and $Gal(F_1/F_0)$ equals the quotient group H_0/H_1, which is cyclic by assumption.

The group $Gal(F_1/F_0) = H_0/H_1$ is cyclic, hence abelian, Lemma 16.12.8 holds, and we can replace the Galois extension $F_0 \subset F_1$ with a chain of intermediate fields where each extension is Galois and of prime degree.

We now use the fact that there is a chain of subgroups $\{1\} = H_k \subset H_{k-1} \subset \cdots \subset H_2 \subset\subset H_1$ (with H_{i+1} normal in H_i, H_i/H_{i+1} cyclic) to inductively show that F_2/F_1, F_3/F_2, etc. are all Galois extension such that Galois groups $Gal(F_2/F_1)$, $Gal(F_3/F_2)$, etc. are all cyclic and we replace each of these with chains of intermediate fields with extensions that are Galois and of prime degree as well. We thus complete a chain from F to K of the desired form, and conclude that $\alpha \in K$, the splitting field for f is solvable. Since all roots of f are in K, we have proved one direction.

We now suppose that all roots of f are solvable. Since the splitting field K is generated by these roots, we know that there is a chain of subfields from F to K where 4ach F_{i+1}/F_i is Galois and of prime degree. Since a group of prime order must be cyclic, and the fact that K/L and L/F are both Galois implies $Gal(K/L)$ is a normal subgroup of $Gal(K/F)$, we simply reverse the argument from above to obtain that $G = Gal(K/F)$ is indeed solvable. This completes the proof.

We see that $Gal(F_{i+1}/F_i)$ is Galois for each extension and since H_i is normal in H_{i+1}, it follows by Theorem 16.7.5 that $Gal(F_{i+1}/F_i)$ and K/F_i is Galois for each intermediate extension. Furthermore, since H_i is

Problems from Chapter 14 of Artin's Algebra:

1.3 $R = \mathbb{Z}[\alpha]$ where α is an algebraic integer. Since α is an algebraic integer, there exists a monic irreducible integer polynomial $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ so that $f(\alpha) = 0$. Here, n is the fixed integer

corresponding to the degree of α over $\mathbb{Q}$. Thus $R \cong \mathbb{Z}[x]/f(x)$. Then, for an integer m, the quotient ring R/mR is isomorphic to $\mathbb{Z}[x]/(f,m) \cong \mathbb{Z}/m\mathbb{Z}[x]/(f) \cong \{a_0 + a_1\alpha + a_2\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Z}/m\mathbb{Z}\}$. Thus R/mR is finite of order m^n.

1.4 (a) Suppose the V is a simple R-module, that is $V \neq 0$ and the only submodules of V are 0 and V itself. We adapt the proof of Proposition 11.3.19 (b) which said that a ring with exactly two ideals in a field.

Since $V \neq 0$, pick a nonzero element $w \in V$. The set $W = \{rw : r \in R\}$ is clearly a nontrivial submodule of V and thus $W = V$ since V is simple. Consequently any simple module V contains a $w \neq 0$ so that the map $\phi_w : R^1 \to V$, defined by multiplication by w, is surjective. Thus, by the First Isomorphism Theorem, Theorem 14.1.6 (c), letting $M = Ker\ \phi_w$, we see that $V \cong R/M$. We finish the result by noting that $M = Ker\ \phi_w$ is an ideal (submodule) of R^1 and if $M' \subset M$ strictly then the Correspondence Theorem, Theorem 14.1.6 (d), says that $\phi_w(M')$ would be a submodule of V strictly containing 0. However V is simple, so $\phi_w(M') = V$, which corresponds to R^1. Thus M must be a maximal ideal as R^1 is the only R-module strictly containing it.

(b) Schur's Lemma says that if $\phi : S \to S'$ is a homomorphism of simple modules, then ϕ is either zero or an isomorphism.

If ϕ is the zero map, then $Ker\ \phi = S$ and $Im\ \phi = 0$.

If ϕ is not the zero map, then $Ker\phi$ is a proper submodule of S, but since S is simple, this implies $Ker\phi = 0$. Thus ϕ is injective. Furthermore, $Im\ \phi \neq 0$ since ϕ is not the zero map, so $Im\ \phi = S'$. Thus ϕ is surjective. Consequently, if ϕ is not the zero map, it is bijective and hence an isomorphism. This concludes the proof of Schur's Lemma.

2.2 Let R be a ring such that every finitely generated R-module is free. This is vacuously try for $R = 0$ so assume $R \neq 0$. We wish to assume that the only possibility left is that R is a field. If R is not a field, then there exists $\alpha \in R$ such that α has no inverse in R. Thus consider the R-module $V = R^1/\alpha R^1$. Then V is generated by x satisfying the relation $\alpha x = 0$. Hence V is finitely generated but not free. Thus we have proven the contrapositive, and a ring R with the described property is indeed the zero ring or a field.

Rem: Note that when R is a field, all finitely generated R-modules are actually vector spaces and have bases, and hence are free. So all fields in fact have the desired property.