

Abstract Algebra Solutions (August 2007)

1. (a) No. Since 3 is a divisor of both 2007 and 123456, the equation

$$2007n + 123456m = 1$$

has no solution with $n, m \in \mathbb{Z}$; equivalently, there is no integer n for which

$$2007n \equiv 1 \pmod{123456}.$$

This shows that $[1] \in \mathbb{Z}_{123456}$ does not lie in the subgroup generated by $[2007]$ in \mathbb{Z}_{123456} .

(b) Let m be the order of a in G , let $q \cdot n_H$ be the largest multiple of n_H which does not exceed m , and put $r = m - q \cdot n_H$; then clearly $0 \leq r < n_H$. Since a^m is the identity of G , and $a^{n_H} \in H$, we have

$$a^r = a^{m-q \cdot n_H} = a^m (a^{q \cdot n_H})^{-1} = ((a^{n_H})^q)^{-1} \in H.$$

In view of the definition of n_H , the integer r cannot be positive since $r < n_H$; therefore, $r = 0$ and $m = q \cdot n_H$. Thus, n_H divides the order of a in G .

(c) A complex number z lies in S^1 if and only if $z = \exp(2\pi i x)$ for some $x \in \mathbb{R}$. Hence, the map $\phi : \mathbb{R} \rightarrow S^1$ given by

$$\phi(x) = \exp(2\pi i x) \quad (x \in \mathbb{R})$$

is a homomorphism from the additive group \mathbb{R} onto the multiplicative group S^1 . Clearly, the kernel of ϕ is \mathbb{Z} . Since $\text{image}(\phi) \cong \mathbb{R}/\ker(\phi)$, it follows that $S^1 \cong \mathbb{R}/\mathbb{Z}$ as required.

2. (a) Let $a \in R$ and $r \in \sqrt{I}$ be arbitrary, and let $n \geq 1$ be such that $r^n \in I$. Since R is commutative and I is an ideal, $(ar)^n = a^n r^n \in I$, which shows that $ar \in \sqrt{I}$. Thus, $R \cdot \sqrt{I} = \sqrt{I}$.

Next, let $r, s \in \sqrt{I}$ and let m, n be positive integers such that $r^m, s^n \in I$. Since R is commutative, we have

$$\begin{aligned} (r + s)^{m+n} &= \sum_{j=0}^{m+n} \binom{m+n}{j} r^{m+n-j} s^j \\ &= r^m \sum_{j=0}^n \binom{m+n}{j} r^{n-j} s^j + s^n \sum_{j=n+1}^{m+n} \binom{m+n}{j} r^{m+n-j} s^{j-n} \\ &= r^m a + s^n b \end{aligned}$$

for some elements $a, b \in R$. Since I is an ideal, $(r + s)^{m+n} \in I$, and thus $r + s \in \sqrt{I}$. This shows that $\sqrt{I} + \sqrt{I} = \sqrt{I}$.

(b) True. Let $a, b \in A$ and suppose that $ab \in P \cap A$. Then, in particular, $a, b \in R$ and $ab \in P$. Since P is a prime ideal in R , either $a \in P$ or $b \in P$; hence, $a \in P \cap A$ or $b \in P \cap A$.

3. (a) Let σ be an automorphism of $\mathbb{Q}[i]$. Since

$$\sigma(0) = \sigma(0 + 0) = \sigma(0) + \sigma(0) = 2\sigma(0),$$

it follows that $\sigma(0) = 0$. Similarly, since σ is not identically zero, the relation

$$\sigma(z) = \sigma(1 \cdot z) = \sigma(1)\sigma(z) \quad (z \in \mathbb{Q}[i])$$

implies that $\sigma(1) = 1$. For every positive integer n we conclude that

$$\sigma(n) = \sigma(\underbrace{1 + \cdots + 1}_{n \text{ copies}}) = \underbrace{\sigma(1) + \cdots + \sigma(1)}_{n \text{ copies}} = \underbrace{1 + \cdots + 1}_{n \text{ copies}} = n.$$

Since

$$0 = \sigma(0) = \sigma(n + (-n)) = \sigma(n) + \sigma(-n) = n + \sigma(-n),$$

we see that $\sigma(-n) = -n$ for every positive integer n .

The arguments above show that \mathbb{Z} is fixed by σ , that is, $\sigma(n) = n$ for all $n \in \mathbb{Z}$. As σ is an automorphism, it follows that \mathbb{Q} (the field of fractions of \mathbb{Z}) is also fixed by σ . Since

$$\sigma(a + bi) = a + b\sigma(i) \quad (a + bi \in \mathbb{Q}[i]),$$

the map σ is therefore determined entirely by the value $\sigma(i)$. Noting that

$$\sigma(i)^2 + 1 = \sigma(i^2 + 1) = \sigma(0) = 0,$$

we see that $\sigma(i) \in \{\pm i\}$, hence there are precisely two distinct automorphisms of $\mathbb{Q}[i]$: if $\sigma(i) = i$, then σ is the identity automorphism, while $\sigma(i) = -i$ corresponds to the automorphism given by complex conjugation.

(b) If $g \in \mathbb{C}[x, y, z, w]$ and $f \in I$, then

$$(gf)(1, 2, 3, 4) = g(1, 2, 3, 4)f(1, 2, 3, 4) = 0,$$

hence $gf \in I$; this shows that $\mathbb{C}[x, y, z, w] \cdot I = I$. Similarly, if $f_1, f_2 \in I$, then

$$(f_1 + f_2)(1, 2, 3, 4) = f_1(1, 2, 3, 4) + f_2(1, 2, 3, 4) = 0,$$

and thus $f_1 + f_2 \in I$; this shows that $I + I = I$. Therefore, I is an ideal of $\mathbb{C}[x, y, z, w]$.

To prove that I is a maximal ideal, it suffices to show that for every element $g \in \mathbb{C}[x, y, z, w]$ which does not lie in I , the ideal generated by I and g contains the unit function $\mathbf{1}$ given by

$$\mathbf{1}(x, y, z, w) = 1 \quad (x, y, z, w \in \mathbb{C}).$$

Let ξ be the number $g(1, 2, 3, 4) \neq 0$, and let $f(x, y, z, w) = 1 - \xi^{-1}g(x, y, z, w)$ for all $x, y, z, w \in \mathbb{C}$. Then $f(1, 2, 3, 4) = 0$, hence $f \in I$, and we have

$$f(x, y, z, w) + \xi^{-1}g(x, y, z, w) = 1 \quad (x, y, z, w \in \mathbb{C}).$$

Therefore, $\mathbf{1} = f + \xi^{-1}g$, and $f + \xi^{-1}g$ lies in the ideal generated by I and g .

4. (a) A permutation is said to be *even* [resp. *odd*] if it can be written as the composition of an even [resp. odd] number of transpositions.

(b) Let $\text{sgn} : S_n \rightarrow \{\pm 1\}$ be the signature homomorphism:

$$\text{sgn}(\sigma) = \begin{cases} +1 & \text{if } \sigma \text{ is even;} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

The restriction sgn_H of sgn to a subgroup H of S_n gives a homomorphism of H into $\{\pm 1\}$. Denoting by H' the set of even permutations in H , we have $H' = \ker(\text{sgn}_H)$. Since $H/H' = H/\ker(\text{sgn}_H) \cong \text{image}(\text{sgn}_H) \subseteq \{\pm 1\}$, we see that $[H : H'] = 1$ or 2 , which implies the result.

(c) Assume that B is another subgroup of order p and $B \neq A$. Consider

$$AB = \{ab \mid a \in A, b \in B\}.$$

We claim that if $ab = a_1b_1$ where $a, a_1 \in A$ and $b, b_1 \in B$, then $a = a_1$ and $b = b_1$. Indeed, if $ab = a_1b_1$, then $a_1^{-1}a = b_1b^{-1}$. Since $a_1^{-1}a \in A$ and $b_1b^{-1} \in B$, we have $a_1^{-1}a = b_1b^{-1} \in A \cap B$. Since A and B are two different subgroups of order p which is a prime number, $A \cap B = \{e\}$ where e denotes the identity element of G . It follows that $a_1^{-1}a = b_1b^{-1} = e$. Hence $a = a_1$ and $b = b_1$.

By the claim, $|AB| = |A| \cdot |B| = p^2 > pq = |G|$. This is impossible.

Linear Algebra Solutions (August 2007)

A. (8 points) Let P_n be the vector space consisting of all the polynomials in the variable x over the rational numbers of degree less than n . Define a linear map $L : P_5 \rightarrow \mathbb{Q}^{2 \times 3}$ by

$$L(f) = \begin{bmatrix} f(1) & 2f(-1) + f(1) & 3f(0) \\ f(1) - f(0) & f(-1) - f(1) & f(0) \end{bmatrix}.$$

(a) Specify a basis for P_5 and a basis for $\mathbb{Q}^{2 \times 3}$.

Solution: A basis for P_5 is $\{1, x, x^2, x^3, x^4\}$. A basis for $\mathbb{Q}^{2 \times 3}$ is the 6 elementary matrices $E_{i,j}$ $i = 1, 2, j = 1, 2, 3$ where $E_{i,j}$ has a 1 in the (i, j) -entry and 0's otherwise.

(b) Find the matrix representing the linear transformation L in the bases for P_5 and $\mathbb{Q}^{2 \times 3}$ you specified in (a).

Solution: We use the obvious ordering on the basis for P_5 and order

the $E_{i,j}$'s as $E_{1,1}, E_{1,2}, E_{1,3}, E_{2,1}, E_{2,2}, E_{2,3}$. Then $L = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 3 & -1 & 3 & -1 & 3 \\ 3 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & -2 & 0 & -2 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$

(c) Using (b) or otherwise, find a basis for the kernel of L and a basis for the image of L .

Solution: The matrix has rank 3 and a basis for the kernel of L is $-x^2 + x^4, -x + x^3$. The first 3 columns of the matrix are linearly independent and so form a basis for the image.

B. (5 points) Let $A \in \mathbb{Q}^{10 \times 10}$ be a diagonal matrix with diagonal entries

$$\{1, 2, 2, 3, 3, 3, 4, 4, 4, 4\}.$$

Let C_A be the space of all matrices $B \in \mathbb{Q}^{10 \times 10}$ which commute with A , that is,

$$C_A = \{B \mid AB = BA\}.$$

What is the dimension of C_A ? Prove your answer.

Solution: A matrix $A = (a_{ij})$ commutes with B if and only if it is a block diagonal matrix with block sizes 1, 2, 3, 4 respectively. The dimension of the space of such matrices is $1^2 + 2^2 + 3^2 + 4^2 = 30$.

C. (5 points) Let A be a square matrix over \mathbb{R} . Assume that the characteristic polynomial of A is x^7 , the rank of A is 4, and the rank of A^2 is 1. Classify all such matrices A up to similarity.

Solution: Since the characteristic polynomial is x^7 the invariant factors are all of the form x^a with $a \leq 7$. The rank of a block corresponding to the cyclic module $k[x]/(x^a)$ is $a-1$ and the rank of the block squared is $a-2$ (or 0 if $a=1$).

Since A^2 has rank 1, all but one block in the canonical decomposition must be of size 2 or smaller with one block of size exactly 3. This reduces the possibilities for the invariant factors to $x, x, x, x, x^3, x, x, x^2, x^3, x^2, x^2, x^3$. However A has rank 4 so the only possible invariant factors are x^2, x^2, x^3 so there is only one similarity class. It has

3 blocks, two of the form $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and one of the form $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$.

D. (6 points) A real $n \times n$ matrix U is called *orthogonal* if $U^{-1} = U^T$ where U^T is the transpose of U .

(a) Prove that if U is orthogonal, then the eigenvalues of U are ± 1 .

Proof: Let v be an eigenvector of U with eigenvalue λ . Then $\lambda|v|^2 = \langle Uv, v \rangle = \langle v, U^T v \rangle$ where $\langle \cdot, \cdot \rangle$ is the standard inner product on \mathbb{R}^n . Since $U^T = U^{-1}$, $U^T v = \lambda^{-1}v$. Thus $\lambda|v|^2 = \lambda^{-1}|v|^2$, so $\lambda^2 = 1$; i.e. $\lambda = \pm 1$.

(b) Prove that the converse is true if in addition, U is symmetric.

Proof: Since $U = U^T$ because U is symmetric, it suffices to show that $U^2 = I$. Since U is symmetric then it is diagonalizable so we can write $U = PAP^{-1}$ with A a diagonal matrix with ± 1 on the diagonal. Thus $A^2 = I$ and hence $U^2 = PIP^{-1} = I$.

E. (6 points) For each of the following statements, state True or False. If true, prove it. If False, give a counter example.

(a) For $A \in \mathbb{R}^{3 \times 3}$, $\det(A+I) = \det(A) + \det(I)$ if $\text{tr}(A) = -\text{tr}(\text{adj}(A))$. (Here I denotes the 3×3 identity matrix, and $\text{tr}(A)$ and $\text{adj}(A)$ denote the trace and adjoint of A respectively.)

Solution: This is TRUE: Let $\lambda_1, \lambda_2, \lambda_3$ be the eigenvalues of A . Then the eigenvalues of $A + I$ are $\lambda_1 + 1, \lambda_2 + 1, \lambda_3 + 1$. Since $A^{-1} = \text{adj}A(\det A)^{-1}$, the eigenvalues of $\text{adj}A$ are the products $\lambda_1\lambda_2, \lambda_1\lambda_3, \lambda_2\lambda_3$, so if we assume that $\text{tr}(A) = -\text{tr}(\text{Adj}A)$ then $\lambda_1 + \lambda_2 + \lambda_3 + \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3 = 0$. Hence $\det(A + I) = (\lambda_1 + 1)(\lambda_2 + 1)(\lambda_3 + 1) = \lambda_1\lambda_2\lambda_3 + 1 = \det(A) + \det I$.

6

(b) A bilinear form on a vector space over the real numbers is positive definite if and only if it is non-degenerate. (A bilinear form \langle, \rangle is *non-degenerate* if for every $\mathbf{v} \neq 0$, there is a vector \mathbf{w} with $\langle \mathbf{v}, \mathbf{w} \rangle \neq 0$.)

Solution: False. Let $V = \mathbb{R}$ and define $\langle a, b \rangle = -ab$.