

# Algebra Problems

Christopher Drupieski

Summer 2005

# Contents

<b>Introduction</b>	<b>ii</b>
<b>1 Groups</b>	<b>1</b>
1.1 General Group Theory . . . . .	1
1.2 Applications of the Sylow Theorems . . . . .	8
1.3 Finite Abelian Groups . . . . .	15
1.4 Additional Results . . . . .	18
<b>2 Rings</b>	<b>19</b>
2.1 Basic Commutative Ring Theory . . . . .	19
Rings of Fractions . . . . .	24
2.2 PIDs, UFDs and Polynomial Rings . . . . .	26
2.3 Non-commutative Rings . . . . .	34
2.4 Additional Results . . . . .	37
<b>3 Modules and Canonical Forms</b>	<b>40</b>
3.1 Modules . . . . .	40
3.2 Rational and Jordan canonical form . . . . .	44
<b>4 Fields</b>	<b>45</b>
4.1 General Field Theory . . . . .	45
4.2 Galois Theory . . . . .	51
4.3 Finding Galois Groups . . . . .	57
<b>5 Multilinear Algebra</b>	<b>63</b>
5.1 Dual spaces and bilinear forms . . . . .	63
5.2 Tensor Products . . . . .	65

# Introduction

The problems appearing in this packet were those provided by Mr. Abramenko to the students preparing for the University of Virginia Mathematics Department Algebra General Exam, Summer 2005. The dates appearing before most of the problems refer to the month and year that problem appeared in a prior General Exam. A few of the results presented in each Additional Results section come from work done in Mr. Abramenko's Algebra 751-752 sequence in Fall 2004-Spring 2005. Each solution is either my own, or else was presented by another participant in the General Exam preparation course. Chapters 3 through 5 were typed by Nicholas Hamblet.

# Chapter 1

## Groups

### 1.1 General Group Theory

1. [May 78 #1] Name a nonabelian simple group.

*Proof.* For  $n \geq 5$ ,  $A_n$  is nonabelian simple. □

2. [Jan 79 #8] Do the elements of finite order in a group always form a subgroup?

*Proof.* No. If  $G = \langle a, b | a^2 = b^2 = e \rangle$ , then  $ab$  is an element of  $G$  of infinite order. So the set of elements of  $G$  of finite order is not closed under multiplication. □

3. [May 89 #5] If  $H, K$  are subgroups of  $G$  show  $G$  is a disjoint union of double cosets  $HgK$ .

*Proof.* Define a relation  $\sim$  on elements of  $G$  by  $g_1 \sim g_2$  if  $\exists h \in H, k \in K$  such that  $g_2 = hg_1k$ . Since  $\sim$  is an equivalence relation,  $G$  splits as a disjoint union of  $\sim$  equivalence classes, i.e., as a disjoint union of double cosets  $HgK$ . □

4. [Feb 84 #7] If  $H, K$  are subgroups of  $G$  with  $Ha = Kb$  for some  $a, b \in G$ , prove  $H = K$ . What can you say if  $aH = Kb$ ?

*Proof.* We have  $Ha = Kb \Rightarrow Hab^{-1} = K$ . Then  $\exists h \in H$  such that  $hab^{-1} = e$ . Then  $ab^{-1} \in H$  (in fact,  $ab^{-1} = h^{-1}$ , so  $K = Hab^{-1} = H$ ). If  $aH = Kb$ , then  $aHb^{-1} = K$ , which implies that  $\exists h \in H$  such that  $ahb^{-1} = e$ . Then  $b^{-1} = h^{-1}a^{-1}$ , so  $K = aHb^{-1} = aHh^{-1}a^{-1} = aHa^{-1}$ . □

5. [Aug 04 #1] Assume that the group  $G$  is a direct product of two finite subgroups  $A$  and  $B$ , and that  $|A|, |B|$  are relatively prime. Show that  $H = (H \cap A) \times (H \cap B)$  for any subgroup  $H \leq G$ .

*Proof.* Clearly  $(H \cap A) \times (H \cap B) \subseteq H$ . Let  $h \in H$ , and let  $n = |A|, m = |B|$ . Since  $G = A \times B$ ,  $\exists a \in A, b \in B$  such that  $h = ab$ . Since  $(n, m) = 1$ ,  $\exists s, t \in \mathbb{Z}$  such that  $ns + mt = 1$ . Now  $h^{mt} = h^{1-ns} = (ab)^{1-ns} = a^{1-ns}b^{1-ns} = aa^{-ns}b^{mt} = a$ . So  $a \in H \cap A$ . Then also  $b \in H \cap B$ , and  $H \subseteq ((H \cap A) \times (H \cap B))$ .  $\square$

6. [Jan 89 #2] (a) If  $G$  has a normal subgroup  $N$  with  $G/N = \mathbb{Z}$ , show for all  $n \neq 0$  there is a normal subgroup  $N_n$  with  $G/N_n = \mathbb{Z}_n$ . (b) If all proper factor groups of  $G/N$  are finite, must  $G$  be finite?

*Proof.* For each  $n \neq 0$ , let  $\overline{N_n}$  be the inverse image of the subgroup  $\mathbb{Z}_n$  under the map  $G/N \rightarrow \mathbb{Z}$ , and let  $N_n$  be the inverse image of  $\overline{N_n}$  under the map  $G \rightarrow G/N$ . Then  $N \leq N_n \trianglelefteq G$  by the Correspondence Theorem, and  $(G/N)/(N_n/N) \cong (\mathbb{Z}/n\mathbb{Z})$ .  $\square$

7. [Aug 89 #1] State the class equation for a finite group. Let  $G$  be a non-trivial p-group. Prove  $Z(G) > 1$ , and prove that  $G$  is nilpotent.

*Proof.* Have  $|G| = |Z(G)| + \sum_{i=1}^n [G : G_{x_i}]$ , where  $\{x_i | 1 \leq i \leq n\}$  are representatives of the distinct non-central conjugacy classes of  $G$  (possibly  $n = 0$ , in which case  $G$  is abelian). If  $G$  is a non-trivial p-group, then  $p \mid |G|$ . Since  $p \mid [G : G_{x_i}]$  for each  $1 \leq i \leq n$ , conclude  $p \mid |Z(G)|$ , hence  $Z(G) \neq \{e\}$ . Assume by induction that any group of order  $p^k$  for  $k < n$  is nilpotent. Let  $G$  be a group of order  $p^n$ . Since  $Z(G) \neq \{e\}$ ,  $G/Z(G)$  is a p-group of order strictly less than  $p^n$ , hence is nilpotent by the induction hypothesis. The center of  $G$  is trivially nilpotent because it is abelian. If  $H \leq Z(G)$ , then  $G$  is nilpotent iff  $H$  and  $G/H$  are nilpotent. Conclude that  $G$  is nilpotent. Hence all finite p-groups are nilpotent.  $\square$

8. [Jan 05 #1] Write down the class equation of the dihedral group  $D_{20}$ . No proof is required by you should identify the terms in your equation.

*Proof.* Write  $D_{20} = \langle \sigma, \tau | \sigma^{10} = \tau^2 = e, \tau\sigma\tau = \sigma^{-1} \rangle$ . Then

$$\begin{aligned} |D_{20}| &= |Z(G)| + |C_\sigma| + |C_\tau| + |C_{\sigma\tau}| + |C_{\sigma^2}| + |C_{\sigma^3}| + |C_{\sigma^4}| \\ &= 2 + 2 + 2 + 2 + 2 + 5 + 5 \end{aligned}$$

$\square$

9. [May 78 #2] If a finite p-group  $G$  acts linearly on a finite-dimensional  $\mathbb{F}_p$ -vector space  $V$ , show  $G$  has a nonzero fixed point.

*Proof.* Let  $n = \dim_{\mathbb{F}_p}(V)$ . Then  $|V| = p^n$ . Let  $\{x_1, x_2, \dots, x_r\}$  be representatives of the distinct  $G$  orbits of  $V$ . Then  $|V| = \sum_{k=1}^r |G \cdot x_k|$ . Since  $G$  acts linearly,  $g \cdot 0 = 0$  for all

$g \in G$ . Without loss of generality, take  $x_1 = 0$ . Observe that  $p \mid |V|$  but  $p \nmid |G \cdot 0|$ , so  $\exists 1 \leq i \leq r$  such that  $p \nmid |G \cdot x_i|$ . Then  $|G \cdot x_i| = 1$ , which implies that  $x_i$  is a non-zero fixed point of  $G$ .  $\square$

10. [Aug 95 #1] Let  $G$  be a finite group of permutations on a finite set  $X$ . For  $x \in X$  let  $G_x = \{g \in G \mid gx = x\}$ . If  $|X| = [G : G_x]$  for some  $x \in X$ , show the same holds for all  $x \in X$ .

*Proof.* Let  $x \in X$  and suppose  $|X| = [G : G_x]$ . Consider the action of  $G$  on  $X$  by  $g \cdot y = g(y)$ . Let  $y \in X$ . Now  $|G \cdot x| = [G : G_x] = |X|$  implies that  $y \in G \cdot x$ , so  $\exists h \in G$  such that  $y = h \cdot x$ . Then  $[G : G_y] = |G \cdot y|$ , and  $G \cdot y = G \cdot (g \cdot x) = Gg \cdot x = G \cdot x$ . Conclude  $[G : G_y] = |G \cdot y| = |X|$ .  $\square$

11. [Aug 99 #2] Show that any finite group  $G$  has a faithful action on some set  $S$  of cardinality  $|S| = |G|$ .

*Proof.* The group  $G$  acts on itself by left multiplication, and this action is faithful because  $gh = h \forall h \in G \Rightarrow g = e$ .  $\square$

12. [Aug 99 #2] Let  $G$  be a finite  $p$ -group for a prime  $p$  having a unique subgroup  $G_p$  for order  $p$ . (a) Show that  $G_p$  is invariant under all endomorphisms of  $G$ . (b) Show that whenever  $G$  acts on a finite set  $S$  of order  $|S| < |G|$ , the subgroup  $G_p$  acts trivially. Conclude that  $G$  can only act faithfully on sets of size  $\geq |G|$ .

*Proof.* (a) If  $f$  is an endomorphism of  $G$ , then  $f(G_p)$  is a  $p$ -subgroup of  $G$ , hence equal to  $G_p$  by the uniqueness of  $G_p$ . (b) We have  $|S| = \sum_{i=1}^n |G : G_{s_i}|$ , where  $\{s_1, \dots, s_n\}$  are representatives of the distinct  $G$ -orbits of  $S$ . Since  $|S| < |G|$ , we must have  $|G_{s_i}| > p$  for each  $1 \leq i \leq n$ . Then each  $G_{s_i}$  contains a subgroup of order  $p$ , i.e.,  $G_p \subseteq G_{s_i}$  for each  $1 \leq i \leq n$ . Conclude that  $G_p$  acts trivially on  $S$ . If  $G$  acts faithfully on a set  $X$ , then the only element which can act trivially on  $X$  is the identity  $\Rightarrow |X| \geq |G|$ .  $\square$

13. [Sep 86 #6] For what  $n$  is  $S_n \rightarrow \text{Aut}(S_n)$  (via  $g \rightarrow \kappa_g$  conjugation by  $g$ ) a monomorphism?

*Proof.* The above map has kernel  $Z(S_n)$ , which is trivial for  $n = 1, n \geq 3$ . For  $n = 2$ , the above map is the trivial map, because  $S_2 \cong \mathbb{Z}_2$ ,  $\text{Aut}(\mathbb{Z}_2) = \{\text{id}\}$ .  $\square$

14. [March 83 #3] Show that  $S_8$  contains a subgroup  $H$  of order 15, but  $S_n$  for  $n < 8$  does not.

*Proof.* By an application of the Sylow Theorems, any group of order 15 is cyclic. If  $g \in S_n$  has order 15, then  $g$  must have both a 5-cycle and a 3-cycle in its disjoint cycle decomposition  $\Rightarrow n \geq 8$ . Now in  $S_8$ ,  $\langle(6\ 7\ 8)\rangle \leq N_{S_8}(\langle(1\ 2\ 3\ 4\ 5)\rangle)$ , so  $H := \langle(6\ 7\ 8)\rangle\langle(1\ 2\ 3\ 4\ 5)\rangle$  is a subgroup of  $S_8$  of order 15.  $\square$

15. [Apr 77 #5] (a) Show the alternating group  $A_n$  is normal in  $S_n$ . (b) Show  $A_n$  is generated by all 3-cycles  $(1\ 2\ k)$  for  $k = 2, 3, \dots, n$ . (c) Show any normal subgroup of  $A_n$  which contains a 3-cycle must be all of  $A_n$ .

*Proof.* (a) Have that  $A_n$  is the kernel of the homomorphism  $\sigma \rightarrow \text{sgn } \sigma$ , hence is normal. (b) and (c) See notes from Algebra I.  $\square$

16. [May 92 #3] Prove  $V = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$  is a normal subgroup of  $S_4$ , and that  $S_4/V \cong S_3$ .

*Proof.* Have  $V = [A_4, A_4] \text{ char } A_4 = [S_4, S_4] \text{ char } S_4$ , hence  $V \trianglelefteq S_4$ . Now  $S_4/V$  is a group of order 6 having three subgroups of order 2 (namely, the subgroups generated by  $(1\ 2)V$ ,  $(1\ 3)V$ , and  $(1\ 4)V$ ), hence is not cyclic. Conclude that  $S_4/V \cong S_3$ .  $\square$

17. [Jan 94 #6] (a) Explain why the automorphism group of  $A_n$  is isomorphic to  $A_n$  for  $n \geq 4$ . (b) Prove that for  $n \geq 3$ ,  $A_n$  has outer automorphisms.

*Proof.* (a) The map  $g \rightarrow \kappa_g$  induces the isomorphism  $A_n/Z(A_n) \cong \text{Inn}(A_n)$ . But  $Z(A_n) = \{e\}$  for  $n \geq 4$ , and the desired isomorphism follows. (b) Consider map  $f : S_n \rightarrow \text{Aut}(A_n)$  given by  $g \mapsto \kappa_g$ . Now  $\ker f$  is a normal subgroup of  $S_n$  having trivial intersection with  $A_n$  for  $n \geq 4$  (by part (a) above). Conclude that  $f$  is injective for  $n \geq 4$ . It is an easy matter to check that  $\kappa_{(1\ 2)}$  is not an inner automorphism of  $S_3$ . We conclude that  $\kappa_{(1\ 2)} \in \text{Aut}(S_n) \setminus \text{Inn}(S_n)$  for  $n \geq 3$ .  $\square$

18. [May 90 #1] If  $G$  has no nontrivial automorphisms, prove it has order 1 or 2.

*Proof.* Let  $G$  be a nontrivial group. If the automorphism  $g \mapsto g^{-1}$  is trivial, then  $g = g^{-1}$  for all  $g \in G$ . Then  $G$  can be considered as a vector space over  $\mathbb{Z}_2$ . Let  $\mathfrak{B}$  be a basis for  $G$  as a  $\mathbb{Z}_2$  vector space. If  $|\mathfrak{B}| > 1$ , then we can construct a nontrivial automorphism of  $G$ . Conclude that  $|\mathfrak{B}| = 1$ , and  $G = \mathbb{Z}_2$ .  $\square$

19. [Jan 87 #2] If  $G$  is infinite but some nontrivial element  $x \neq 1$  has only a finite number of conjugates, show  $G$  is not simple.

*Proof.* By assumption,  $n := [G : C_x] < \infty$ , where  $C_x = \{g \in G : gxg^{-1} = x\}$ . Consider the permutation representation of the group action of  $G$  on the set of left cosets of  $C_x$ . We have a homomorphism  $\varphi : G \rightarrow G/C_x$ , where here  $G/C_x$  denotes the set of left cosets of  $C_x$  in  $G$ . Then  $\ker \varphi$  is a normal subgroup of  $G$  of finite index.  $\square$

20. [Jan 04 #1] Let  $G = \{g_1, \dots, g_n\}$  be a finite abelian group. Show that the product  $P := g_1 \cdots g_n$  is of order 1 or 2.

*Proof.* If  $g \in G$  is an element of order  $> 2$ , then  $g \neq g^{-1}$ , so we may group together and cancel out all elements in  $P$  of order  $> 2$ . Now since  $G$  is abelian, after cancelling either  $P = e$  or  $\text{ord}(P) = 2$ .  $\square$

21. [May 92 #5] Use the subgroup structure of the cyclic group of order  $n \geq 1$  to show that  $n = \sum_{d|n} \phi(d)$ , where  $\phi$  is the Euler  $\phi$ -function.

*Proof.* The group  $G$  decomposes as a disjoint union  $G = \dot{\cup}_{d|n} \{g \in G : \text{ord}(g) = d\}$ . Let  $g \in G$  be an element of order  $d \mid n$ . The set of generators of the subgroup  $\langle g \rangle$  is the set  $\{g^k : 1 \leq k \leq d, (k, d) = 1\}$ , which has cardinality  $\phi(d)$ . Cyclic groups have unique subgroups of order  $d$  for each  $d \mid n$ . Conclude that if  $h$  is an element of  $G$  of order  $d$ , then  $h$  is a generator of  $\langle g \rangle$ . Now  $|G| = \sum_{d|n} |\{g \in G : \text{ord}(g) = d\}| = \sum_{d|n} \phi(d)$  by the remarks above.  $\square$

22. [Jan 95 #5] Give definitions of the terms “maximal subgroup” and “minimal subgroup”. Then from your definitions prove the following facts: (a) A minimal subgroup must be cyclic of prime order. (b) If a subgroup has prime index, it is a maximal subgroup. (c) If a subgroup is both maximal and normal, it has prime index. (d) A subgroup of an abelian group is maximal iff it has prime index. (e) Find all maximal and all minimal subgroups of  $\mathbb{Z}$ .

*Proof.* A nontrivial subgroup  $H \leq G$  is maximal if there are no proper subgroups of  $G$  containing  $H$ . A nontrivial subgroup  $H \leq G$  is minimal if there are no nontrivial subgroups contained in  $H$ .

- (a) Let  $G$  be a group, and let  $H \leq G$  be a minimal subgroup. Let  $h \in H \setminus \{e\}$ . If  $\text{ord}(h) = \infty$ , then  $\langle h^2 \rangle$  is a proper nontrivial subgroup of  $H$ . So  $\text{ord}(h) < \infty$  for all  $h \in H$ . If  $\langle h \rangle \neq H$ , then  $\langle h \rangle$  is a proper nontrivial subgroup of  $H$ . Let  $n = \text{ord}(h)$ . If  $p$  is a nontrivial factor of  $n$ , then  $\langle h^{n/p} \rangle$  is a proper nontrivial subgroup of  $H$ . Conclude that  $H$  must be cyclic of prime order.

- (b) Let  $M \leq G$  be a subgroup of prime index  $p$ . If  $M \leq H \leq G$ , then  $[G : H] \mid p$ , which implies that either  $[G : H] = 1$  ( $G = H$ ) or  $[G : H] = p$ , in which case we must have  $[H : M] = 1$  ( $H = M$ ). Then  $M$  is maximal.
- (c) Let  $M$  be a normal subgroup of  $G$  of prime index. Then  $G/M$  is cyclic of prime order, which implies that  $G/M$  has no nontrivial subgroups. Then by the Correspondence Theorem there are no proper subgroups of  $G$  containing  $M$ , which implies that  $M$  is maximal.
- (d) Follows from parts (b) and (c).
- (e) By part (d), the maximal subgroups of  $\mathbb{Z}$  are  $p\mathbb{Z}$  for  $p$  prime. Since  $\mathbb{Z}$  has no cyclic subgroups of finite order, it has no minimal subgroups by part (a).  $\square$

23. [Aug 95 #7] Find the order of the group  $GL_n(\mathbb{F}_p)$  and describe one of its  $p$ -Sylow subgroups.

*Proof.* Have

$$\begin{aligned} |GL_n(\mathbb{F}_p)| &= (p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1}) \\ &= p^{n-1}p^{n-2} \cdots p^2 p (p^n - 1)(p^{n-1} - 1) \cdots (p - 1) \end{aligned}$$

So a  $p$ -Sylow subgroup of  $GL_n(\mathbb{F}_p)$  will have order  $p^e$ , where  $e = \sum_{j=1}^{n-1} j = \frac{n(n-1)}{2}$ .  $\square$

24. [Aug 98 #2] (a) Find the order  $n$  of the group  $GL_2(p)$  for  $p$  prime. (b) For  $\lambda \in \mathbb{F}_p$ , and

$$B = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$$

find the order  $m$  of the subgroup  $G_\lambda := \{A \in GL_2(\mathbb{F}_p) : ABA^{-1} = B\}$ . (c) Find how many  $2 \times 2$  matrices over  $\mathbb{F}_p$  are similar to the matrix  $B$ .

*Proof.* (a) By the previous problem,  $|GL_2(\mathbb{F}_p)| = p(p-1)(p^2-1)$ . (b) Simple calculations show that  $A = ((a, b)(c, d)) \in GL_2(\mathbb{F}_p)$  commutes with  $B$  iff  $a = d \neq 0$  and  $c = 0$ . Then  $m = p(p-1)$ . (c) Considering the group action of  $GL_2(\mathbb{F}_p)$  on  $B$  by conjugation, we know that the number of matrices similar to  $B$  is equal to the index  $[G : G_\lambda] = p^2 - 1$ .  $\square$

25. [Aug 96 #1] A Hall subgroup of a finite group  $G$  is a subgroup whose order and index are relatively prime. Prove that if  $N \trianglelefteq G$  and  $H \leq G$  is a normal subgroup of  $G$ , then  $HN/N$  is a Hall subgroup of  $G/N$  and  $H \cap N$  is a Hall subgroup of  $N$ .

*Proof.* Note that  $|H| = |H \cap N| |HN : N|$ , and  $[G : H] = [N : H \cap N] [G/N : HN/N]$ . If  $(|H|, [G : H]) = 1$ , then also  $(|H \cap N|, [N : H \cap N]) = 1$  and  $(|HN/N|, [G/N : HN/N]) = 1$ .  $\square$

26. [Aug 97 #2] (a) Prove that if  $G$  is a finite group with exactly two conjugacy classes of elements, then  $|G| = 2$ . (b) If  $G$  has exactly three conjugacy classes of elements, show that  $|G|$  involves at most two primes. (c) There are, in fact, only two finite groups with exactly three conjugacy classes of elements. Can you guess which ones they are?

*Proof.* (a) Let  $G$  be a finite group with exactly two conjugacy classes of elements,  $C_1$  and  $C_2$ . Say  $C_1 = \{e\}$ . If  $|G|$  is divisible by two distinct primes  $p$  and  $q$ , then  $\exists x, y \in G$  such that  $\text{ord}((\ )x) = p$  and  $\text{ord}((\ )y) = q$ . Moreover, every element in the  $G$  conjugacy class of  $x$  will have  $p$ -power order, and every element in the conjugacy class of  $y$  will have  $q$ -power order. But  $x, y \in C_2$ , a contradiction, because  $y$  is not of  $p$ -power order. So  $|G| = p^k$  for some  $k \in \mathbb{N}$ . Now  $|C_2| = p^k - 1$  and  $|C_2| \mid |G| = p^k$ . From these two conditions we conclude  $p^k = 2$ . (b) Let  $G$  be a finite group with exactly three conjugacy classes of elements. If  $|G|$  is divisible by three distinct primes  $p, q, r$ , then a similar argument as in part (a) leads to a contradiction. (c)  $S_3$  and  $\mathbb{Z}_3$  each have exactly three conjugacy classes of elements.  $\square$

27. [Sep 93 #7] A well-known puzzle has tiles numbered 1 to 15 in 4 rows of 4 each, with the  $(4, 4)$  square empty. An allowable move consists of sliding a tile adjacent to the empty square horizontally or vertically into the empty square. If a sequence of moves ends up with the empty square back at  $(4, 4)$ , prove the resulting permutation  $\pi$  of the numbers 1 to 15 belongs to  $A_{15}$ .

*Proof.* Given any ordering of the pieces on the board we have an element of  $S_{15}$ : Reading the numbers from left to right, top to bottom, and ignoring the empty space, suppose the numbers 1 to 15 occur in the order  $i_1, i_2, \dots, i_{15}$ . Then we have the permutation given by  $j \mapsto i_j$ . Evidently sliding the empty space left or right does not affect the permutation. Let  $b$  denote the blank spot, and suppose at some point in the game the pieces appear in the order  $i_1, i_2, \dots, i_j, b, i_{j+1}, \dots, i_{15}$ . Let  $\sigma$  denote the corresponding permutation. Suppose we can move the blank spot down. Then the new ordering is given by  $i_1, i_2, \dots, i_j, i_{j+4}, i_{j+1}, i_{j+2}, i_{j+3}, b, i_{j+5}, \dots, i_{15}$ . Then the new permutation  $\tau$  is given by  $(i_{j+1} \ i_{j+4} \ i_{j+3} \ i_{j+2})\sigma$ , i.e., multiplication by an odd permutation. By a similar argument, moving the blank spot up also results in a change in the ordering by an odd permutation. Since any sequence of moves which returns the blank spot to the bottom right corner must involve an even number of vertical moves, the permutation resulting from such a sequence of moves must be the product of an even number of odd permutations, i.e., must be in  $A_{15}$ .  $\square$

28. [Aug 01 #1] If  $\phi : G_1 \rightarrow G_2$  is a homomorphism of groups, and  $N_1 \trianglelefteq G_1$ ,  $N_2 \trianglelefteq G_2$ , show that  $\bar{\phi} : G_1/N_1 \rightarrow G_2/N_2$  is a well-defined homomorphism of quotient groups iff the original homomorphism satisfies  $\phi(N_1) \subseteq N_2$ .

*Proof.* Easy. □

## 1.2 Applications of the Sylow Theorems

1. A group of order  $p^k$  is nilpotent.

*Proof.* See §1.1 #7. □

2. [May 90 #2] A group of order  $441 = 3^2 7^2$  is solvable.

*Proof.* Have  $n_3 \mid 3^2$  and  $n_7 \equiv 1 \pmod{7}$ , so  $n_7 = 1$ . Then  $G$  has a normal subgroup  $P$  of order 49. Now  $G/P$  is a group of order  $3^2$ , and  $p$ -groups are solvable. Since  $P \trianglelefteq G$  is solvable and  $G/P$  is solvable, we conclude that  $G$  is solvable. □

3. [Sep 86 #2] Find all groups of order 99.

*Proof.* Let  $G$  be a group of order 99. By the Sylow Theorems,  $G$  has normal Sylow subgroups of orders  $3^2$  and 11. Conclude that  $G$  is the direct product of its Sylow subgroups, and  $G \cong \mathbb{Z}_{11} \times \mathbb{Z}_9$ , or  $G \cong \mathbb{Z}_{11} \times \mathbb{Z}_3 \times \mathbb{Z}_3$ . □

4. [Nov 77 #7] Must a group of order 70 be abelian? Solvable? Can you say anything about its normal subgroups?

*Proof.* By the Sylow Theorems,  $G$  has normal Sylow subgroups  $P_5$  and  $P_7$  of orders 5 and 7. Then  $G$  has a normal (cyclic) subgroup  $N = P_5 P_7$  of order 35. Since  $G/N$  is cyclic of order 2,  $G/N$  is solvable, which implies that  $G$  is solvable because  $N$  is solvable. The Dihedral group  $D_{70}$  of order 70 is a nonabelian group of order 70. Any proper normal subgroup of  $D_{70}$  of order divisible by 2 would have a characteristic Sylow subgroup of order 2, and hence  $D_{70}$  would have a normal subgroup of order 2, a contradiction. Conclude that a group of order 70 may have normal subgroups of orders 1, 5, 7, 35, 70, but not necessarily of orders 2, 10, or 14. □

5. [Jan 98 #1a] What can you say about groups of the following orders? (a)  $2^4 + 1 = 17$  (b)  $2^3 + 1 = 9$

*Proof.* (a) Any group of prime order is cyclic. (b) Any group of order  $p^2$  is isomorphic to one of  $\mathbb{Z}_{p^2}$ ,  $\mathbb{Z}_p \times \mathbb{Z}_p$ . □

6. [Sep 82 #6] If  $G$  is nonabelian of order 21, show that it is generated by elements  $s, t$  with  $s^7 = t^3 = 1, t^{-1}st = s^2$ .

*Proof.* Let  $G$  be a nonabelian group of order 21. By the Sylow Theorems,  $G$  has a normal subgroup of order 7, and by Cauchy's Theorem,  $G$  has a subgroup of order 3. Then  $G = \mathbb{Z}_7 \rtimes \mathbb{Z}_3$ , and the generator of  $\mathbb{Z}_3$  acts on the generator of  $\mathbb{Z}_7$  by conjugation through some homomorphism  $\varphi : \mathbb{Z}_3 \rightarrow \text{Aut}(\mathbb{Z}_7) \cong \mathbb{Z}_6$ . Say  $\mathbb{Z}_7 = \langle s \rangle$  and  $\mathbb{Z}_3 = \langle t \rangle$ . Since  $G$  is not abelian,  $\varphi$  is nontrivial. The only two elements of  $\text{Aut}(\mathbb{Z}_7)$  of order 3 are the maps  $s \mapsto s^2$  and  $s \mapsto s^4$ . But these are inverse automorphisms, so without loss of generality, we can assume that  $t \cdot s = t^{-1}st = s^2$  (otherwise replace  $t$  as a generator of  $\mathbb{Z}_3$  by  $t^{-1}$ ). Now have  $G$  generated by elements  $s, t$  with  $s^7 = t^3 = 1$  and  $t^{-1}st = s^2$ .  $\square$

7. [Aug 98 #1ab] Let  $G$  be a finite group of order  $3 \cdot 5 \cdot 17$ . Show that the Sylow 17-subgroup is normal. If there exists an element of order 15 in  $G$ , show that the Sylow 3- and 5-subgroups are also normal.

*Proof.* By the Sylow Theorems,  $G$  has a normal Sylow subgroup of order 17. Suppose  $G$  contains an element  $g$  of order 15. Let  $P_3, P_5$  be subgroups of  $\langle g \rangle$  of orders 3 and 5, respectively. Then  $P_3, P_5$  are each Sylow subgroups of  $G$ , and each is normalized by  $\langle g \rangle$ . Have  $n_3 \equiv 1 \pmod{3}, n_3 \mid [G : N_G(P_3)] \in \{1, 7\}$ ;  $n_5 \equiv 1 \pmod{5}, n_5 \mid [G : N_G(P_5)] \in \{1, 7\}$ . Conclude that  $n_3 = n_5 = 1$ .  $\square$

8. [Jan 02 #2] Consider the following two statements: (a) Any group of order 455 is abelian. (b) Any group of order 455 is solvable but there exist nonabelian groups of order 455. Decide which of the two statements is true and prove it.

*Proof.* Let  $G$  be a group of order 455. By the Sylow Theorems we conclude that  $G$  has normal Sylow subgroups  $P_7, P_{13}$  of orders 7 and 13, respectively, and by Cauchy's theorem  $G$  has a subgroup of order 5. By the Sylow Theorems any group of order  $7 \cdot 13$  is cyclic. Conclude that  $G = \mathbb{Z}_{91} \rtimes \mathbb{Z}_5$  for some homomorphism  $\varphi : \mathbb{Z}_5 \rightarrow \text{Aut}(\mathbb{Z}_{91}) \cong \text{Aut}(\mathbb{Z}_7) \times \text{Aut}(\mathbb{Z}_{13}) \cong \mathbb{Z}_6 \times \mathbb{Z}_{12}$ . Since  $(5, 6 \cdot 12) = 1$ , conclude that  $\varphi$  is the trivial homomorphism. Then  $G$  must be abelian. (And any abelian group is solvable.)  $\square$

9. If  $G$  and its normal subgroup  $N$  have the same power of  $p$ , then all  $p$ -Sylow subgroups of  $G$  live in  $N$ ; if one is normal in  $N$ , then it is the unique  $p$ -Sylow subgroup of  $G$ .

*Proof.* Let  $G$  be a finite group,  $N \trianglelefteq G$  a normal subgroup of order divisible by the same power of  $p$  as  $|G|$ . Let  $P \in \text{Syl}_p(G)$ . Then  $P \in \text{Syl}_p(N)$ , and for all  $g \in G, gPg^{-1} \subseteq gNg^{-1} = N$ . Conclude that all Sylow subgroups of  $G$  are contained in  $N$ . If  $P \trianglelefteq N$ , then  $P \text{ char } N \trianglelefteq G$ , which implies that  $P \trianglelefteq G$ , and hence  $|\text{Syl}_p(G)| = 1$ .  $\square$

10. If a normal subgroup  $H$  of  $G$  contains a Sylow subgroup  $P$  of  $G$ , then  $G = HN_G(P)$ .

*Proof.* Since  $H \trianglelefteq G$ ,  $HN_G(P) \leq G$ . Note that  $gPg^{-1} \subseteq gHg^{-1} = H$  for all  $g \in G$ , i.e., all Sylow  $p$ -subgroups of  $G$  are contained in  $H$ , hence are also Sylow  $p$ -subgroups of  $H$ . Let  $g \in G$ . Then  $gPg^{-1}$  is conjugate in  $H$  to  $P$ , i.e.,  $\exists h \in H$  such that  $gPg^{-1} = hPh^{-1}$ . Then  $h^{-1}gPg^{-1}h = P$ , i.e.,  $h^{-1}g \in N_G(P)$ . Now  $g = h(h^{-1}g) \in HN_G(P)$ . Conclude that  $G \subseteq HN_G(P)$ , and thus  $G = HN_G(P)$ .  $\square$

11. [Jan 82 #7bc] The Frattini Subgroup  $F$  of  $G$  is defined to be the intersection of all maximal subgroups of  $G$ . Show: (a)  $F \trianglelefteq G$ . (b) If  $G$  is finitely generated then  $F$  is inessential ( $G = FH \Rightarrow G = H$ ). (c) If  $F$  contains a  $p$ -Sylow subgroup of  $G$ , then that subgroup is normal.

*Proof.*

(a) If  $M \leq G$  is a maximal subgroup of  $G$  and  $\varphi \in \text{Aut}(G)$ , then  $\varphi(M)$  is a maximal subgroup of  $G$ . Conclude that the set of maximal subgroups of  $G$  is invariant under all automorphisms of  $G$ , which implies that their intersection is also invariant under automorphisms of  $G$ . Then  $F \text{ char } G \Rightarrow F \trianglelefteq G$ .

(b) Say  $G = \langle g_1, \dots, g_n \rangle$ . Let  $H \leq G$  such that  $G = FH$ . Suppose  $G \neq H$ . Then by a possible reordering,  $\{g_1, \dots, g_j\} \cap H = \emptyset$  for some  $1 \leq j \leq n$ . Since  $G = FH$ , for each  $1 \leq k \leq j$ ,  $\exists f_k \in F, h_k \in H$  such that  $g_k = f_k h_k$ . Then  $G = \langle g_1, \dots, g_j, H \rangle = \langle f_1, \dots, f_j, H \rangle$ . Since  $H < G$  and because  $G$  is finitely generated, by the usual Zorn's Lemma argument we have that  $H$  is contained in some maximal subgroup  $M \leq G$ . Then  $G = \langle f_1, \dots, f_k, H \rangle \subseteq \langle f_1, \dots, f_k, M \rangle = M$ , since  $f_1, \dots, f_k \in M$ . But  $M \neq G$ , a contradiction. Conclude that  $G = H$ .

(c) Let  $P \in \text{Syl}_p(G)$ , and suppose  $P \subseteq F$ . Then by the previous problem we have  $G = FN_G(P)$ , which implies by part (b) that  $N_G(P) = G$ , i.e.,  $P \trianglelefteq G$ .  $\square$

12. A member  $g$  of a group  $G$  is called a nongenerator of  $G$  if whenever  $G$  is generated by a subset containing  $G$ , it is also generated by the subset with  $g$  removed. It is a fact that the set of all nongenerators of  $G$  forms a subgroup, the Frattini subgroup of  $G$ . If  $F$  is the Frattini subgroup of a finite  $p$ -group  $G$  ( $p$  prime), show that  $g \in F$  iff  $g$  is in every subgroup of index  $p$  of  $G$ . Conclude that  $G/F$  is an abelian group of exponent  $p$ .

*Proof.* Note that the maximal subgroups of  $G$  are precisely the subgroups of index  $p$ . Suppose that  $g$  is an element of every subgroup of index  $p$ . Let  $X \subseteq G$ , and suppose  $G = \langle g, X \rangle$  but  $G \neq \langle X \rangle$ . Have that  $\langle X \rangle$  is contained in some maximal (index  $p$ ) subgroup  $M$  of  $G$ . Then

$G = \langle g, X \rangle \subseteq \langle g, M \rangle = M$ , a contradiction because  $M \neq G$ . Conclude that  $\langle X \rangle = G$ . Now let  $g \in F$ . Let  $M$  be an index  $p$  (hence maximal) subgroup of  $G$ . Suppose  $g \notin M$ . Then we must have  $G = \langle g, M \rangle$ . But  $g \in F \Rightarrow \langle g, M \rangle = M$ . Then  $G = M$ , a contradiction. Conclude that  $g \in M$ .

Every  $p$ -Group is nilpotent, and if  $H$  is a proper subgroup of the nilpotent group  $G$ , then  $H < N_G(H)$ . Let  $M$  be an index  $p$  subgroup of  $G$ . Then  $M \trianglelefteq G$ . Moreover,  $[G : M] = p \Rightarrow G/M \cong \mathbb{Z}_p$ , an abelian group. Conclude that  $[G, G] \leq M$ . Also,  $G/M \cong \mathbb{Z}_p \Rightarrow (gM)^p = M$  for all  $g \in G$ , i.e.,  $G^p \subseteq M$ . Since this is true for all index  $p$  subgroups of  $G$ , we conclude that  $[G, G] \leq F$ , and  $G^p \subseteq F$ . Then  $G/F$  is abelian of exponent  $p$ .  $\square$

13. [Fall 87 #1] If  $G$  of order 160 has two distinct subgroups of order 80, then  $G$  has a normal subgroup of order 5.

*Proof.* Let  $H, K \leq G$  be distinct subgroups of order 80. Each of  $H, K$  is of index 2, hence normal. Then  $HK$  is a subgroup of  $G$  of order strictly greater than 80, which implies that  $G = HK$ . Now from the order formula  $|HK||H \cap K| = |H||K|$ , we conclude that  $|H \cap K| = 40$ . By the Sylow Theorems,  $H \cap K$  has a normal subgroup  $P$  of order 5. Then  $P \text{ char } H \cap K \trianglelefteq H$ , which implies that  $P \trianglelefteq H$ , which implies  $P \text{ char } H \trianglelefteq G$ , which implies that  $P \trianglelefteq G$ .  $\square$

14. [Aug 04 #2] Let  $G$  be a group of order 56, and let  $P_p \in \text{Syl}_p(G)$  for  $p \in \{2, 7\}$ . (a) Show that one of  $P_2, P_7$  is normal in  $G$ . (b) Give an example of a group  $G$  with  $|G| = 56$  and  $P_2$  nor normal in  $G$ . (c) Show that there exists a group of order 56 with non-normal  $P_7$ .

*Proof.*

(a) Have that  $n_7 \in \{1, 8\}$ , and  $n_2 \in \{1, 7\}$ . Suppose  $n_7 = 8$  and  $n_2 = 7$ . Then  $G$  has at least  $8 \cdot 6 = 48$  distinct elements of order 7, and at least  $7 + 4 = 11$  distinct elements of 2-power order, i.e.,  $|G| \geq 48 + 11 = 59 > 56$ , a contradiction. Conclude that one of  $n_7, n_2$  equals 1.

(b) The Dihedral group  $D_{56}$  has no normal subgroup of order 8.

(c) Let  $H = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ . Note that  $\text{Aut}(H) \cong GL_3(\mathbb{F}_2)$ , a group of order 168. Since  $7 \mid 168$ ,  $\exists \sigma \in \text{Aut}(H)$  with  $\text{ord}(\sigma) = 7$ . Then  $H \rtimes_{\sigma} \mathbb{Z}_7$  is a group of order 56 with no normal subgroup of order 7.  $\square$

15. [Aug 98 #1c] If all Sylow subgroups of a finite group  $G$  are normal and abelian, show that  $G$  itself is abelian.

*Proof.* Since each Sylow subgroup of  $G$  is normal, we can establish inductively that  $G$  is the direct product of its Sylow subgroups, and the direct product of abelian groups is abelian.  $\square$

16. [Jan 81 #5] (a) If  $G$  of order 60 has exactly 4 elements of order 5, then  $G$  is not simple. (b) If  $G$  of order 60 has more than 4 elements of order 5, then  $G$  is simple (and hence isomorphic to  $A_5$ ).

*Proof.*

- (a) Have that  $n_5 \mid 12$  and  $n_5 \equiv 1 \pmod{5}$ , which implies that  $n_5 \in \{1, 6\}$ . By the assumption we can conclude that  $n_5 = 1$ , and  $G$  contains a normal subgroup of order 5.
- (b) Let  $G$  be a group of order 60 with more than 4 elements of order 5. Then  $n_5 = 6$ . Suppose  $G$  is not simple. Let  $H$  be a nontrivial normal subgroup of  $G$ . If  $5 \mid |H|$ , then  $H$  contains a Sylow 5-subgroup of  $G$ , and hence  $H$  contains all 6 Sylow 5-subgroups of  $G$  because it is normal. Then  $|H| \geq 6 \cdot 4 + 1 = 25$ , which implies that  $|H| = 30$ . Now, every group of order 30 contains a (cyclic) subgroup of order 15, and hence a normal Sylow 5-subgroup. Then there exists a normal Sylow 5-subgroup  $P_5$  of  $H$ , and  $P_5 \text{ char } H \trianglelefteq G$ , which implies that  $P_5 \trianglelefteq G$ , which implies that  $G$  has only four elements of order 5, a contradiction. So  $5 \nmid |H|$ . Then  $|H| \in \{2, 3, 4, 6, 12\}$ . But in each of these cases,  $G/H$  has a normal subgroup  $\bar{N}$  of order 5. (Apply the Sylow theorems to groups of orders 30, 20, 15, 10 and 5.) Taking the preimage of  $\bar{N}$  under the map  $G \rightarrow G/H$ , we obtain a normal subgroup of  $G$  of order divisible by 5, a contradiction to the above remarks. Conclude that  $G$  is simple.  $\square$

17. [Jan 92 #4] If a finite group  $G$  has normal  $p$ -Sylow subgroup  $P$ , then  $\phi(P) \subseteq P$  for every endomorphism  $\phi$  of  $G$ .

*Proof.* For every endomorphism  $\phi$  of  $G$ , we have that  $\phi(P)$  is a  $p$ -subgroup of  $G$ , hence is contained in some element of  $\text{Syl}_p(G)$ . But  $\text{Syl}_p(G) = \{P\}$ .  $\square$

- 18 [Jan 94 #4] Let  $f : G \rightarrow H$  be a surjective homomorphism of finite groups, and let  $p$  be a prime. (a) Prove that if  $P \in \text{Syl}_p(G)$ , then  $f(P) \in \text{Syl}_p(H)$ . (b) Prove that every  $Q \in \text{Syl}_p(H)$  has the form  $f(P)$  for some  $P \in \text{Syl}_p(G)$ .

*Proof.* (a) Write  $|G| = p^e m$ ,  $p \nmid m$ ,  $|\ker f| = p^j n$ ,  $j \leq e$ ,  $p \nmid n$ ,  $n \mid m$ . Let  $P \in \text{Syl}_p(G)$ . Then  $|f(P)| = [G : P \cap \ker f]$ . We have that  $|P \cap \ker f| \mid p^j$ , and  $|f(P)| \mid |H| = [G : \ker f] = p^{e-j}(m/n)$ . Together these conditions imply that  $|f(P)| = p^{e-j}$ , and hence  $f(P)$  is a  $p$ -subgroup of  $H$  of maximal  $p$ -power, i.e.,  $f(P) \in \text{Syl}_p(H)$ . (b) Let  $Q \in \text{Syl}_p(H)$ , and

let  $Q'$  be the inverse isomorphic image of  $Q$  under the isomorphism  $G/\ker f \cong H$ . By the Correspondence Theorem, there exists a subgroup  $K \leq G$  containing  $\ker f$  such that  $Q'$  is the image of  $K$  under the map  $G \rightarrow G/\ker f$ . Then  $p^e \mid |K|$ . Let  $P \in \text{Syl}_p(K)$ . Then  $P \in \text{Syl}_p(G)$ , and by (a),  $f(P) \in \text{Syl}_p(H)$ . But  $f(P) \subseteq Q$ , which implies that  $f(P) = Q$ .  $\square$

19. [Aug 94 #1] Let  $P$  be a  $p$ -Sylow subgroup of a finite group  $G$ ,  $p$  a prime dividing the order of  $G$ . (a) Prove that  $P$  consists of all the  $p$ -torsion elements of  $N_G(P)$ . (b) Prove that  $P \text{ char } N_G(P)$ . (c) Prove that  $N_G(N_G(P)) = N_G(P)$ .

*Proof.* (a) and (b) Since  $P \trianglelefteq N_G(P)$ ,  $P \text{ char } N_G(P)$  by the Sylow Theorems. Now if  $g \in N_G(P)$  has  $p$ -power, then  $g$  is contained in some element of  $\text{Syl}_p(N_G(P)) = \{P\}$ . (c) Clearly  $N_G(P) \subseteq N_G(N_G(P))$ . Now  $P \text{ char } N_G(P) \trianglelefteq N_G(N_G(P))$ , which implies that  $P \trianglelefteq N_G(N_G(P))$ , which implies  $P \text{ char } N_G(N_G(P))$ . Let  $g \in N_G(N_G(P))$ . Then  $\kappa_g \in \text{Aut}(N_G(P))$ , which implies that  $\kappa_g(P) = P$ , and hence  $g \in N_G(P)$ . Thus  $N_G(N_G(P)) = N_G(P)$ .  $\square$

20. [Aug 96 #8] Give an example of two finite groups whose Sylow subgroups are isomorphic for each prime, but which are not themselves isomorphic.

*Proof.*  $S_3$  and  $\mathbb{Z}_3$ .  $\square$

21. [Jan 97 #6] Let  $P \in \text{Syl}_p(G)$ . Prove that if  $H \leq G$ , then  $H \cap gPg^{-1} \in \text{Syl}_p(H)$  for some  $g \in G$ .

*Proof.* Let  $Q \in \text{Syl}_p(H)$ . Then  $Q \leq gPg^{-1}$  for some  $g \in G$ . Now  $H \cap gPg^{-1}$  is a  $p$ -subgroup of  $H$  containing  $Q$ , hence is must be equal to  $Q$ .  $\square$

22. [May 91 #4b] If  $G$  is a group of order 231, show the 11-Sylow subgroup  $H$  of  $G$  is normal in  $G$  and lies in  $Z(G)$ .

*Proof.* By the Sylow Theorems,  $n_7 = n_{11} = 1$ . Let  $P_7 \in \text{Syl}_7(G)$ . Then  $P_7 \times H \cong P_7H \leq G$ , and  $P_7 \leq C_G(h)$  for each  $h \in H$ . Also,  $H \cong \mathbb{Z}_{11}$ , so  $H \leq C_G(h)$  for each  $h \in H$ . Then  $[G : C_G(h)] = 3$  for each  $h \in H \setminus Z(G)$ . Consider the conjugation action of  $G$  on  $H$ . We have  $|H| = |H \cap Z(G)| + \sum_{i=1}^n [G : C_G(h_i)]$ , where the  $h_i$  are representatives of the noncentral conjugacy classes in  $H$ . Now  $|H \cap Z(G)| \mid 11$ , so  $H \subseteq Z(G)$  or  $H \cap Z(G) = \{e\}$ . Suppose  $H \cap Z(G) = \{e\}$ . Then necessarily  $n > 1$ , and  $|H| - |H \cap Z(G)| = 10 = \sum i = 1^n [G : C_G(h_i)] = 3n$ , a contradiction because  $3 \nmid 10$ . Conclude  $H \subseteq Z(G)$ .  $\square$

23. Show that if  $N_G(P) \subseteq M \subseteq G$  for a  $p$ -Sylow subgroup  $P$  of a finite group  $G$ , then  $[G : M] \equiv 1 \pmod{p}$ .

*Proof.* We have that  $[G : N_G(P)] = [G : M][M : N_G(P)] = [G : M][M : N_M(P)]$  because  $N_G(P) \leq M$ . By the Sylow theorems,  $[G : N_G(P)] \equiv [M : N_M(P)] \equiv 1 \pmod{p}$ . Conclude that  $[G : M] \equiv 1 \pmod{p}$ .  $\square$

24. [Jan 00 #5] Let  $G$  be a finite group such that every element commutes with its conjugates (for any  $g, h \in G$ , the elements  $h$  and  $hgh^{-1}$  commute).

- (a) Show that any Sylow subgroup of such a  $G$  is normal.
- (b) Explain why the group of quaternions  $\{\pm 1, \pm i, \pm j, \pm k\}$  is such a group  $G$ .

*Proof.*

- (a) Let  $p$  be a prime and write  $|G| = p^n m$ ,  $p \nmid m$ . If  $n = 0$ , then  $\text{Syl}_p(G) = \{e\} \trianglelefteq G$ . Suppose that  $|\text{Syl}_p(G)| = 1$  for all groups  $G$  satisfying the hypotheses of the theorem when  $|G|$  can be written in the form  $p^k m$ ,  $p \nmid m$ , with  $k < n$ . Let  $G$  be a group of order  $p^n m$ , and let  $g \in G$  with  $\text{ord}(g) = p$ . Let  $N = \langle \{xgx^{-1} | x \in G\} \rangle$ . Note that if  $x \in G$ , then  $(xgx^{-1})^{-1} = x^{-1}g^{-1}x = x^{-1}g^{p-1}x$ , and  $xg^kx^{-1} = (xgx^{-1})^k$ . Thus every element  $y \in N$  can be written in the form  $y = (x_1gx_1^{-1})(x_2gx_2^{-1}) \cdots (x_rgx_r^{-1})$  for some  $x_1, x_2, \dots, x_r \in G$ . (It now follows almost trivially that  $N \trianglelefteq G$ .) Because the  $xgx^{-1}$  commute,

$$\begin{aligned} y^p &= (x_1gx_1^{-1})^p(x_2gx_2^{-1})^p \cdots (x_rgx_r^{-1})^p \\ &= (x_1g^px_1^{-1})(x_2g^px_2^{-1}) \cdots (x_rg^px_r^{-1}) \\ &= (x_1x_1^{-1})(x_2x_2^{-1}) \cdots (x_rx_r^{-1}) \\ &= e \end{aligned}$$

Then  $N$  is a  $p$ -subgroup of  $G$ . Say  $|N| = p^j$ ,  $1 < j \leq n$ . Consider the quotient group  $G/N$ . Have  $|G/N| = p^{n-j}m$ ,  $n - j < n$ . Also, given  $g, h \in G$ , the elements  $hN$  and  $ghg^{-1}N$  of  $G/N$  commute because the elements  $h, ghg^{-1} \in G$  commute. Then by the induction hypothesis,  $|\text{Syl}_p(G/N)| = 1$ . Let  $\bar{P} \in \text{Syl}_p(G/N)$ . So  $\bar{P} \trianglelefteq G/N$ . By the Correspondence Theorem, there exists a normal subgroup  $P \trianglelefteq G$ ,  $N \leq P$ , such that  $\bar{P} = P/N$ . Then  $|P| = |\bar{P}||N| = p^n$ , so  $P \in \text{Syl}_p(G)$ . But  $P \trianglelefteq G$ , so  $|\text{Syl}_p(G)| = 1$ . Conclude that if  $G$  is a finite group such that every element commutes with its conjugates, then any Sylow subgroup of  $G$  is normal.

- (b) In  $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ , the conjugates of  $\pm 1$  are  $\pm 1$ , the conjugates of  $\pm i$  are  $\pm i$ , the conjugates of  $\pm j$  are  $\pm j$ , and the conjugates of  $\pm k$  are  $\pm k$ . Since  $+g$  and  $-g$  commute  $\forall g \in Q_8$ ,  $Q_8$  satisfies the hypotheses of the theorem.  $\square$

25. [Aug 03 #7] Let  $G$  be a finite group of order  $n$ . Suppose that for every  $d \mid n$ , the equation  $x^d = 1$  has at most  $d$  solutions in  $G$ . Show that: (a) For each prime  $p \mid n$ ,  $|\text{Syl}_p(G)| = 1$ . (b) The Sylow  $p$ -subgroups of  $G$  are cyclic. (c)  $G$  is cyclic.

*Proof.* (a) Suppose  $p \mid |G|$ . Write  $|G| = p^e m$ ,  $p \nmid m$ ,  $e \geq 1$ . If  $|\text{Syl}_p(G)| > 1$ , then the equation  $x^{p^e} = 1$  has at least  $p^e + 1$  solutions. Conclude  $|\text{Syl}_p(G)| = 1$ . (b) Let  $P \in \text{Syl}_p(G)$ . If  $P$  is not cyclic, then the equation  $x^{p^{e-1}} = 1$  has at least  $p^e$  solutions. Conclude that  $P$  is cyclic. (c) Since each Sylow subgroup is normal,  $G$  is the direct product of its Sylow subgroups. Then  $G$  is a direct product of cyclic groups of relatively prime orders, hence  $G$  is cyclic.  $\square$

### 1.3 Finite Abelian Groups

1. Describe (up to isomorphism) all abelian groups of order: 4851, 2334, 200, 72, 1984, 80, 375.

*Proof.*  $\square$

2. How many nonisomorphic abelian groups are there of order: 1776, 360.

*Proof.*  $\square$

3. [Mar 83 #6] Show a finite abelian group is cyclic iff it has no subgroup isomorphic to  $B \oplus B$  for  $B \neq 0$ .

*Proof.* Every subgroup of a cyclic group is cyclic, but a subgroup of the form  $B \oplus B$  for  $B \neq 0$  finite abelian is not cyclic (in particular, every element has order at most  $|B| < |B|^2 = |B \oplus B|$ ). Conversely, let  $G$  be a non-cyclic finite abelian group with invariant factors  $a_1, a_2, \dots, a_n$ , with  $a_i \mid a_{i+1}$  for  $1 \leq i \leq n - 1$ . In particular, we must have  $n > 1$ . So  $G \cong \mathbb{Z}_{a_1} \oplus \dots \oplus \mathbb{Z}_{a_{n-1}} \oplus \mathbb{Z}_{a_n}$ . Since  $a_{n-1} \mid a_n$ ,  $G$  has distinct cyclic subgroups of order  $a_{n-1}$  corresponding to subgroups of the  $\mathbb{Z}_{a_{n-1}}$  and  $\mathbb{Z}_{a_n}$  factors. So  $G$  has a subgroup isomorphic to  $\mathbb{Z}_{a_{n-1}} \oplus \mathbb{Z}_{a_{n-1}}$ .  $\square$

4. [Aug 98 #1d] If  $G$  is a finite abelian group of order  $pqr$  for distinct primes  $p, q, r$ , show that  $G$  is cyclic.

*Proof.* By Cauchy's Theorem,  $G$  has subgroups  $H_p \cong \mathbb{Z}_p, H_q \cong \mathbb{Z}_q, H_r \cong \mathbb{Z}_r$ . Since  $G$  is abelian,  $H_p \times H_q \times H_r \cong H_p H_q H_r \leq G$  is a subgroup of  $G$  of order  $pqr$ , i.e.,  $G \cong H_p \times H_q \times H_r$ , and the direct product of cyclic groups of relatively prime orders is cyclic.  $\square$

5. [May 78 #6] Give an example of a torsion-free abelian group which is not free. Can you give an example which is finitely generated?

*Proof.* The group  $(\mathbb{Q}, +)$  is torsion free but not free, because any two non-zero elements are linearly dependent over  $\mathbb{Z}$ . By the structure theorem of finitely generated modules over a PID, any finitely generated torsion-free abelian group is automatically free.  $\square$

6. [Apr 77 #3] Show that the multiplicative group of the ring  $\mathbb{Z}_p^n$  for prime  $p$ ,  $n > 1$  has a subgroup of order  $p$ .

*Proof.* For  $p$  odd,  $|\mathbb{Z}_p^n| = (p - 1)p^{n-1}$ , and the result is true by Cauchy's Theorem. For  $p = 2$  and  $n \geq 2$ ,  $|\mathbb{Z}_p^n| = 2 \cdot 2^{n-2}$ , and the result follows again by Cauchy's Theorem.  $\square$

7. [Aug 89 #6] Find the structure of all abelian groups generated by 3 elements  $a, b, c$  satisfying the relations  $-4a + 2b + 6c = 0$ ,  $-6a + 2b + 6c = 0$ ,  $7a + 4b + 15c = 0$ .

*Proof.*  $\square$

8. [Jan 98 #2] Take the free abelian group on three generators  $x, y, z$  and divide by the relations  $2x + 4y + 5z = 0$ ,  $6x + 8y + 10z = 0$ ,  $8x + 12y + 20z = 0$ . Write the resulting group as a direct sum of cyclic groups.

*Proof.*  $\square$

9. [Aug 95 #3] Find the order of the abelian group generated by  $x, y, z$  subject to the relations  $4x - 2y + 4z = 0$ ,  $7x - 8y + z = 0$ ,  $8x + y + 13z = 0$ .

*Proof.*  $\square$

10. [Aug 04 #5] Let  $N$  be the  $\mathbb{Z}$ -submodule of  $\mathbb{Z}^3$  generated by the column vectors  $(2, 2, -2)^t$ ,  $(-4, -2, 4)^t$ , and  $(2, 4, 4)^t \in \mathbb{Z}^3$ . (a) Determine the structure of the abelian group  $\mathbb{Z}^3/N$ . (b) Determine a basis  $y_1, y_2, y_3$  of  $\mathbb{Z}^3$  and natural numbers  $d_1 \mid d_2 \mid d_3$  such that  $d_1y_1, d_2y_2, d_3y_3$  is a  $\mathbb{Z}$ -basis for  $N$ .

*Proof.*  $\square$

11. [Jan 97 #2] Let  $G$  be a finite abelian group of order  $k$ . Use the fact that the map  $g \mapsto g^n$ ,  $n \in \mathbb{Z}$ , is a homomorphism to show that if  $k_n$  is the number of solutions of  $g^n = 1$  in  $G$  and  $k^{(n)}$  is the number of  $n$ -th powers of in  $G$ , then  $k = k_n k^{(n)}$ .

*Proof.* The map  $f : g \mapsto g^k$  establishes the isomorphism  $G/\ker f \cong G^k$ . Now  $|\ker f| = k_n$ , and  $k^{(n)} = |G^k|$ , and the result follows.  $\square$

12. [Aug 96 #2] Determine all pairs of positive integers  $a, b$  with  $a \leq b$  such that  $\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_{15} \times \mathbb{Z}_{18} \times \mathbb{Z}_{20}$ .

*Proof.* Let  $G = \mathbb{Z}_{15} \times \mathbb{Z}_{18} \times \mathbb{Z}_{20}$ . Observe that  $G \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5$ . Claim: The only possible values for  $a$  and  $b$  are (i)  $a = 2 \cdot 3 \cdot 5$ ,  $b = 4 \cdot 9 \cdot 5$ , and (ii)  $a = 4 \cdot 3 \cdot 5$ ,  $b = 2 \cdot 9 \cdot 5$ . Reasoning: These are the only possible combinations as long as both  $a$  and  $b$  are each divisible by each of 2, 3, 5. Since  $\mathbb{Z}_{p^3} \not\cong \mathbb{Z}_p \times \mathbb{Z}_{p^2}$  and  $\mathbb{Z}_{p^2} \not\cong \mathbb{Z}_p \times \mathbb{Z}_p$ , if all of the elementary divisors of  $G$  corresponding to one of 2, 3, 5 appear in one of  $a, b$ , then we cannot recover the decomposition  $G \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5$ .  $\square$

13. [Aug 94 #2] If  $G$  is a finite abelian group of order  $n$ , show that  $G$  has a subgroup of order  $d$  for each divisor  $d$  of  $n$ . Show that this need not be true if  $G$  is abelian.

*Proof.* First one establishes Cauchy's Theorem for finite abelian groups: If  $p$  prime divides the order of the finite abelian group  $G$ , then  $G$  contains an element of order  $p$ . Then one establishes the desired result by induction on the group order. The simple group  $A_5$  has no subgroup of order 30 because any such subgroup would be normal.  $\square$

14. [Aug 99 #3] The exponent  $e$  of a group  $G$  is defined as the smallest positive integer  $k$  such that  $x^k = 1$  for all  $x \in G$ . If  $n_1, n_2, \dots, n_r$  are the invariant factors of a finite abelian group  $A$  ( $n_1 \mid n_2 \mid \dots \mid n_r$ ), prove that  $A$  has exponent  $e = n_r$ , and has an element of order precisely  $e$ . Conclude that  $A$  has an element of order  $m$  iff  $m$  divides the largest invariant factor  $n_r$ .

*Proof.* We know that  $A$  has a cyclic subgroup of order  $n_r$ , so the generator of that subgroup is an element of order precisely  $e = n_r$ . Given  $g = (a_1, a_2, \dots, a_r) \in \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r} \cong A$ , we have that  $g^{n_r} = (a_1^{n_r}, a_2^{n_r}, \dots, a_r^{n_r}) = 1$ , because  $\text{ord}(a_i) \mid n_i$  and  $n_i \mid n_r$  for each  $1 \leq i \leq n_r$ .  $\square$

15. [Jan 92 #1] Show that an infinite abelian group is cyclic iff every nonzero subgroup has finite index.

*Proof.* Let  $G$  be an infinite cyclic abelian group. Then  $G \cong \mathbb{Z}$ , and we know that every subgroup of  $\mathbb{Z}$  has finite index. Now let  $G$  be an infinite abelian group such that every nonzero subgroup has finite index. Let  $g \in G$ , and  $n := [G : \langle g \rangle]$ . Let  $x_1, \dots, x_n$  be representatives of the  $\langle g \rangle$ -cosets of  $G$ . Then  $G = \langle g, x_1, \dots, x_n \rangle$ , i.e.,  $G$  is finitely generated. Now we apply the structure theorem for finitely generated abelian groups to show that  $G \cong \mathbb{Z}$ .  $\square$

16. [Aug 98 #3] For an abelian group  $A$ , the dual group  $A^*$  is defined to be  $\text{Hom}(A, S)$ , where  $S$  denotes the multiplicative group of complex numbers of modulus 1, and  $\text{Hom}(A, B)$

denotes the abelian group of homomorphisms from  $A$  into  $B$  (group operation is pointwise addition/multiplication). Using the property  $\text{Hom}(A_1 \oplus A_2, B) \cong \text{Hom}(A_1, B) \oplus \text{Hom}(A_2, B)$ , prove (a)  $\mathbb{Z}_n^* \cong \mathbb{Z}_n$  (b)  $A^* \cong A$  for any finite abelian group  $A$ .

*Proof.* (a) If  $f \in \text{Hom}(\mathbb{Z}_n, S)$ , then  $f$  is completely determined by its value on the generator  $g$  of  $\mathbb{Z}_n$ . Also,  $f$  must map  $g$  to an  $n$ -th root of unity. So  $|\mathbb{Z}_n^*| \leq n$ , because there are only  $n$  such roots, and each root determines a different element of  $\mathbb{Z}_n^*$ . Let  $\zeta$  be a primitive  $n$ -th root of unity, and let  $f : \mathbb{Z}_n \rightarrow S$  satisfy  $g \mapsto \zeta$ . Then  $f \in \mathbb{Z}_n^*$ , and  $\text{ord}(f) = n$ . Conclude that  $\mathbb{Z}_n^*$  is cyclic of order  $n$ , generated by  $f$ . (b) This follows by applying the structure theorem for finitely generated abelian groups to write  $A$  as a direct sum of cyclic subgroups, and then by applying the hint along with part (a).  $\square$

## 1.4 Additional Results

**Problem.** Prove or disprove: (a)  $S_{11}$  has a subgroup of order 33. (b)  $S_{11}$  has a subgroup of order 55.

**Solution.**

(a) Let  $G$  be a group of order 33,  $n_{11} := |\text{Syl}_{11}(G)|$ ,  $n_3 := |\text{Syl}_3(G)|$ ,  $P_{11} \in \text{Syl}_{11}(G)$ ,  $P_3 \in \text{Syl}_3(G)$ . Then  $n_{11}|3$ ,  $n_{11} \equiv 1 \pmod{11} \Rightarrow n_{11} = 1$ , and  $n_3|11$ ,  $n_3 \equiv 1 \pmod{3} \Rightarrow n_3 = 1$ . Conclude that  $G \cong P_3 \times P_{11} \cong \mathbb{Z}_3 \times \mathbb{Z}_{11} \cong \mathbb{Z}_{33}$ . Then  $S_{11}$  contains a subgroup of order 33 iff it contains an element of order 33. Suppose  $g \in S_n$  is a permutation of order 11. The order of a permutation is the least common multiple of the lengths of the cycles in its disjoint cycle decomposition. Then in its disjoint cycle decomposition,  $g$  must contain both a 3-cycle and an 11-cycle, which implies that  $n \geq 14$ . Conclude that  $S_{11}$  has no subgroup of order 33.

(b) Let  $a = (1\ 2\ 3 \cdots 10\ 11)$ ,  $b = (2\ 4\ 10\ 6\ 5)(3\ 7\ 8\ 11\ 9)$ . Note that  $bab^{-1} = a^3 \in \langle a \rangle$ , so  $b \in N_{S_{11}}(\langle a \rangle)$ . Then  $\langle a \rangle \langle b \rangle \leq S_{11}$ , and  $|\langle a \rangle \langle b \rangle| = \frac{|a||b|}{|\langle a \rangle \cap \langle b \rangle|} = |a||b| = 55$ , where  $|\langle a \rangle \cap \langle b \rangle| = 1$  because  $(|a|, |b|) = 1$ .

# Chapter 2

## Rings

### 2.1 Basic Commutative Ring Theory

1. [1985 #3c] If  $a, b$  are relatively prime integers, show the ring  $\mathbb{Z}_{ab}$  is isomorphic to the direct sum  $\mathbb{Z}_a \oplus \mathbb{Z}_b$ . Show (in  $\leq 1$  word) why this implies if  $m = p^{e_1} \cdots p^{e_t}$  that  $\mathbb{Z}_m \cong \mathbb{Z}_{p^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{e_t}}$ .

*Proof.* The map  $\mathbb{Z}_{ab} \rightarrow \mathbb{Z}_a \oplus \mathbb{Z}_b$  defined by  $x + (ab) \mapsto (x + (a), x + (b))$  is a well-defined injective ring homomorphism. Because the domain and range of the map are both finite sets, we conclude that the map is also a bijection, and hence an isomorphism. The general result follows by induction.  $\square$

2. [May 92 #2] If  $a, b$  in an integral domain  $R$  satisfy  $a^n = b^n$ ,  $a^m = b^m$  for  $m, n$  relatively prime, show  $a = b$ . (Do you need that  $R$  is an integral domain?)

*Proof.* Let  $F$  denote the field of fractions of  $R$ . Then in  $F$ ,  $(\frac{a}{b})^n = 1 = (\frac{a}{b})^m$ . So in  $F$ ,  $\text{ord}(\frac{a}{b})$  divides both  $m$  and  $n$ , from which we conclude that  $\frac{a}{b} = 1$  in  $F$ , and hence  $a = b$  in  $R$ .

Consider the ring  $R = \mathbb{Q}[x, y]$ , and the ideal  $I = (x^2 - y^2, x^3 - y^3)$  of  $R$ . Now  $x - y \in I \Rightarrow \exists f, g \in R$  such that  $x - y = (x^2 - y^2)f + (x^3 - y^3)g = (x - y)((x + y)f + (x^2 + xy + y^2)g)$ . Then applying the cancellation property in an integral domain, we have  $1 = (x + y)f + (x^2 + xy + y^2)g$ , i.e.,  $1 \in (x, y)$ , ( $\Rightarrow \Leftarrow$ ) because  $(x, y)$  is a maximal ideal. Note also, we can write  $I$  as a product of ideal  $I = (x - y)(x + y, x^2 + xy + y^2) = (x - y)(x + y, x^2, xy, y^2)$ . So  $(x - y)^3 = (x - y)(x^2 - 2xy + y^2) \in I$ . Then  $R/I$  is ring which is not an integral domain,  $x + I \neq y + I$ ,  $x^2 + I = y^2 + I$ , and  $x^3 + I = y^3 + I$ .  $\square$

3. [Feb 84 #3] If  $R$  is finite, show every prime ideal is maximal.

*Proof.* Let  $P \subseteq R$  be a prime ideal. Then  $R/P$  is a finite integral domain  $\Rightarrow R/P$  is a field  $\Rightarrow P$  is a maximal ideal.  $\square$

4. [Sep 93 #2] If  $P$  is a prime ideal which is not maximal, show  $P$  has infinitely many cosets in  $R$ .

*Proof.* Let  $P \subseteq R$  be a prime ideal. If  $P$  has only finitely many cosets in  $R$ , then  $R/P$  is a finite integral domain, hence a field, which implies that  $P$  is a maximal ideal ( $\Rightarrow \Leftarrow$ ). Conclude that  $P$  has infinitely many cosets in  $R$ .  $\square$

5. [May 90 #5] If  $R$  is an integral domain with only a finite number of ideals, show  $R$  is a field, and give an upper bound for  $n$ .

*Proof.* Let  $a \in R \setminus \{0\}$ . Consider the chain of ideals  $(a) \supseteq (a^2) \supseteq \dots$ . Since  $R$  has only finitely many ideals, this chain must stabilize. Then for some  $j \geq 1$ ,  $(a^j) = (a^{j+1})$ . Then  $\exists r \in R$  such that  $ra^{j+1} = a^j$ , which implies by the cancellation property of integral domains that  $ra = 1$ , i.e.,  $a$  is a unit. So  $R$  is a field. In this case,  $R$  has at most two distinct ideals:  $R$  and  $\{0\}$ .  $\square$

6. [Jan 92 #6] Prove that an integral domain has the descending chain condition on ideals iff it is a field.

*Proof.* If  $R$  is an integral domain having the descending chain condition on ideals, then  $R$  is a field by the argument in the previous exercise. If  $R$  is a field, then it trivially has the descending chain condition on ideals.  $\square$

7. [Jan 94 #8] Let  $ZD$  denote the set of zero divisors of  $R$  (including 0). Let  $\mathcal{I}$  be the set of ideals of  $R$  which are contained in  $ZD$ . (a) Show that  $R \setminus ZD$  is closed under multiplication. (b) Show that if  $M$  is a maximal member of  $\mathcal{I}$ , then  $M$  is a prime ideal. (c) Use Zorn's Lemma to show that each member of  $ZD$  is contained in a maximal member of  $\mathcal{I}$ . (d) Conclude that  $ZD$  is a union of prime ideals.

*Proof.*

(a) Let  $a, b \in R \setminus ZD$ . If  $c \in R \setminus \{0\}$  is such that  $abc = 0$ , then either  $bc = 0$  ( $\Rightarrow \Leftarrow$ ), or  $a$  is a zero divisor ( $\Rightarrow \Leftarrow$ ). Conclude that  $R \setminus ZD$  is multiplicatively closed.

(b) Let  $a, b \in R$ , and suppose  $ab \in M$  but  $a \notin M$ ,  $b \notin M$ . Then each of the ideals  $(a)+M$ ,  $(b)+M$  must contain an element which is not a zero divisor. Say  $ra+m_1$ ,  $sb+m_2$  are not zero divisors for  $r, s \in R$ ,  $m_1, m_2 \in M$ . Then  $(ra+m_1)(sb+m_2) = rs(ab) + ram_2 + sbm_1 + m_1m_2 \in M \cap (R \setminus ZD)$  ( $\Rightarrow \Leftarrow$ ). Conclude that  $M$  is prime.

(c) Let  $m \in M$  be nonzero. Then  $(m)$  is a proper ideal of  $R$  contained in  $ZD$ . Apply the usual Zorn's Lemma argument to the collection  $\mathcal{J}$  of ideals of  $R$  contained in  $ZD$ .

(d) By part (c), each  $z \in ZD$  is contained in some maximal (hence prime by part (b)) member  $M_z$  of  $\mathcal{I}$ . Then  $ZD = \cup_{z \in ZD} M_z$ .  $\square$

8. [Jan 82 #6] If  $I$  is an ideal of  $R$  with  $I \cap S = \emptyset$  for some multiplicatively closed subset  $S$  of  $R$  containing 1, show there exists an ideal  $M$  of  $R$  containing  $I$  and maximal with respect to  $M \cap S = \emptyset$ . Find an  $M$  if  $R = \mathbb{Z}$ ,  $S = \{3^n : n \geq 0\}$ ,  $I = 2\mathbb{Z}$ .

*Proof.* The result follows from the usual Zorn's Lemma argument. The ideal  $I = 2\mathbb{Z}$  is already maximal, so  $M = I$ .  $\square$

9. [Sep 78 #6] A ring  $R$  is called a local ring if it has a unique maximal ideal. A domain is called a valuation domain if for every two elements  $a, b$ , either  $a \mid b$  or  $b \mid a$ . (a) Show that  $R$  is a local ring iff the non-units of  $R$  form an ideal  $M$ . (b) Show that every valuation domain is local. (c) Show that a local ring has no idempotent ( $e^2 = e$ ) other than 1,0.

*Proof.*

(a) Suppose the non-units of  $R$  form an ideal  $M$ . Then  $M$  is maximal, for any ideal properly containing  $M$  contains a unit, hence must be  $R$ . If  $M'$  is another maximal ideal of  $R$ , then necessarily  $M' \subseteq R \setminus R^*$ . If  $M' \neq M$ , then  $M$  is a proper ideal of  $R$  properly containing  $M'$  ( $\Rightarrow \Leftarrow$ ). Conclude  $M' = M$ . Conversely, suppose  $R$  has a unique maximal ideal  $M$ . Clearly  $M \subseteq R \setminus R^*$ . If  $c \in R \setminus R^*$ , then by Zorn's Lemma ( $c$ ) is contained in some maximal ideal of  $R$ . So  $c \in M$ , which implies  $M = R \setminus R^*$ .

(b) Let  $R$  be a valuation domain. It is clear that the set of non-units of  $R$  is closed under multiplication by elements of  $R$ . Let  $a, b \in R$ , and assume  $a \mid b$ . Write  $b = ra$  for some  $r \in R$ . Now if  $1 = (a + b)u = a(1 + r)u$  for some  $u \in R$ , then  $a \in R^*$ . So the set of non-units of  $R$  must also be closed under addition. Then the set of non-units of  $R$  forms an ideal, and hence  $R$  is local by part (a).

(c) Suppose  $a \in R$  is a nontrivial idempotent. Then  $0 = a - a^2 = a(1 - a)$ . Each of  $a, 1 - a$  is a zero divisor of  $R$ , there exist maximal ideals  $M_1, M_2$  of  $R$  with  $a \in M_1$ ,  $1 - a \in M_2$ . Moreover,  $M_1 \neq M_2$ , or else  $1 = (1 - a) + a$  is contained in a maximal ideal of  $R$ . Conclude that  $R$  is not a local ring.  $\square$

10. [Aug 97 #8] (a) Show that the set  $N$  of all nilpotent elements of  $R$  forms an ideal (called the nilradical of  $R$ ). (b) The intersection  $J$  of all maximal ideals of  $R$  is called the Jacobson radical of  $R$ . Show that  $N \subseteq J$ . (c) Give an example where  $N$  and  $J$  are different.

*Proof.* (a) If  $a, b \in N$ ,  $r \in R$ ,  $a^n = 0$ ,  $b^m = 0$ , then  $(ra)^n = 0$  and  $(a + b)^{n+m} = 0$  by the Binomial Theorem. So  $N$  is an ideal. (b) Let  $M$  be a maximal ideal, and let  $a \in N$ . Say  $a^n = 0$ . Maximal ideals are prime ideals, so  $a^n = 0 \in M \Rightarrow a \in M$ . Then  $N \subseteq M$  for all maximal ideals  $M$ , and hence  $N \subseteq J$ . (c) Let  $R = \mathbb{Z}$ ,  $P = 2\mathbb{Z}$ ,  $S = R \setminus P$ . Consider the local ring  $R_P = S^{-1}R$ . This ideal has a single nonzero maximal ideal, but no nonzero nilpotent elements. So  $N = \{0\} \subsetneq M = J$ .  $\square$

11. [May 89 #7] Show an element  $a \in R$  belongs to  $J = \cap\{\text{maximal ideals of } R\}$  iff  $1 + ra$  is a unit for all  $r \in R$ .

*Proof.* Let  $a \in R$ , and suppose  $1 + ra \notin R^*$  for some  $r \in R$ . Then  $(1 + ra)$  is contained in some maximal ideal  $M$  of  $R$ . Now  $a \in J \subseteq M \Rightarrow ra \in M \Rightarrow 1 = (1 + ra) - ra \in M (\Rightarrow \Leftarrow)$ , because  $M$  is a proper ideal. So  $a \in J \Rightarrow 1 + ra \in R^*$ , for all  $r \in R$ . Conversely, suppose  $a \notin J$  for some maximal ideal  $M$ . Then  $(a) + M = R$ , so  $\exists r \in R, m \in M$  such that  $ra + m = 1$ . Then  $1 - ra = m \notin R^*$ . So  $1 + ra \in R^*$  for all  $r \in R \Rightarrow a \in J$ .  $\square$

12. [May 78 #5] Is the ring  $C[0, 1]$  of continuous real-valued functions on the closed interval  $[0, 1]$  noetherian?

*Proof.* No. For  $n \geq 1$ , let  $I_n = \{f : [0, 1] \rightarrow \mathbb{R} : f(x) = 0 \forall x \in [0, 1/n]\}$ . Then  $I_1 \subseteq I_2 \subseteq \dots$  is an infinite increasing chain of ideals which does not stabilize. Hence  $C[0, 1]$  is not Noetherian.  $\square$

13. [Sep 79 #7a] Give two examples of non-noetherian rings.

*Proof.* The ring  $C[0, 1]$  of continuous real-valued functions on the closed interval  $[0, 1]$  is not noetherian by the above remarks. Given a field  $F$ , the polynomial ring  $F[x_1, x_2, \dots]$  in infinitely many variables is a non-noetherian ring because it has the infinite strictly increasing chain of ideals  $(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset \dots$ .  $\square$

14. [May 80 #2] Hilbert's Theorem says that  $F[x_1, \dots, x_n]$  is noetherian. Show that any finitely generated commutative  $F$ -algebra  $A$  is noetherian.

*Proof.* Let  $A$  be a finitely generated  $F$ -algebra. Then  $\exists a_1, \dots, a_n \in A$  such that  $A = F[a_1, \dots, a_n]$ . We have an  $F$ -homomorphism  $\phi : F[x_1, \dots, x_n] \rightarrow A$  mapping  $x_i \mapsto a_i$ . The homomorphic image of a noetherian ring is noetherian. Conclude that  $A$  is noetherian.  $\square$

15. [Aug 99 #4] If  $R$  is an integral domain, find all  $R$ -linear automorphisms of the polynomial ring  $R[x]$ .

*Proof.* Let  $\phi$  be an  $R$ -linear automorphism of  $R[x]$ . Then  $\phi$  is completely determined by its value on  $x \in R[x]$ . Say  $\phi(x) = g(x)$  where  $\deg(g) = n$ . Observe that  $\deg(\phi(f)) = n \deg(f)$  for all  $f \in R[x]$ . If  $n = 0$  then  $\phi(R[x]) \subseteq R (\Rightarrow \Leftarrow)$ . If  $n \geq 2$  then  $x \notin \phi(R[x])$ . Conclude that  $n = 1$ . Say  $\phi(x) = ax + b$  for some  $a, b \in R$ , and say  $cx + d = \phi^{-1}(x)$  for some  $c, d \in R$ . Then  $x = a(cx + d) + b = (ac)x + (ad + b) \Rightarrow ac = 1 \Rightarrow a \in R^*$ . Now, given any  $ax + b \in R[x]$  with  $a \in R^*$ , there exists an  $R$ -linear homomorphism  $\varphi : R[x] \rightarrow R[x]$  mapping  $x \mapsto ax + b$ . (For existence, consider the injection  $R[x] \hookrightarrow R[x][y]$  and the evaluation homomorphism  $R[x][y] \rightarrow R[x]$  given by the map  $y \mapsto ax + b$ .) If  $\varphi(f) = 0$ , then  $\deg f = 0 \Rightarrow f \in R \Rightarrow f = 0$ , so  $\varphi$  is injective. And  $\varphi(a^{-1}(x - b)) = x$ , so  $\varphi$  is surjective, and hence an automorphism.  $\square$

16. [Mar 83 #8] Does 7 divide  $10^{31} + 31^{10}$ ? Why?

*Proof.* Reducing the expression modulo 7, we have  $10^{31} + 31^{10} \equiv 3^{31} + 3^{10} \equiv 3 \cdot (3^2)^{15} + (3^2)^5 \equiv 3 \cdot 2^{15} + 2^5 \equiv 3 \cdot (2^3)^5 + 4 \cdot 8 \equiv 3 + 4 = 7 \equiv 0 \pmod{7}$ . So  $7 \mid 10^{31} + 31^{10}$ .  $\square$

17. [Apr 77 #4] (a) If  $M \trianglelefteq R$  is a maximal ideal, show  $R/M$  is a field. (b) If  $R$  is a Euclidean domain, show every ideal generated by an irreducible element is maximal.

*Proof.* (a) Easy. (b) Recall that Euclidean  $\Rightarrow$  PID. Also, the principal ideal generated by an irreducible element is always maximal among principal ideals.  $\square$

18. [Sep 93 #5] (a) Let  $D$  be a Euclidean domain, with Euclidean function  $\delta$ . Let  $D_n = \{a \in D : a \neq 0 \text{ and } \delta(a) \geq n\}$ . Show that (i) if  $b \in D_0$  and there exists an  $a \in D$  such that  $a + Db \subseteq D_n$ , then  $b \in D_{n+1}$ ; (ii)  $\bigcap_n D_n = \emptyset$ . (b) Conversely, show that if an integral domain  $D$  has a chain of subsets  $D \setminus \{0\} = D_0 \supseteq D_1 \supseteq D_2 \supseteq \dots$  satisfying (i) and (ii), then  $D$  is Euclidean.

*Proof.*

(a) Have  $0 \notin D_n \forall n \geq 0$ , and given  $d \in D \setminus \{0\}$ , we have  $d \notin D_n$  for  $n \geq \delta(d)$ . So  $\bigcap_n D_n = \emptyset$ . Let  $a, b \in D, b \neq 0$  and suppose  $a + Db \subseteq D_n$ . Since  $D$  is Euclidean,  $\exists q, r \in D$  such that  $a = bq + r$  and  $r = 0$  or  $\delta(r) < \delta(b)$ . Now  $r = a - qb \in a + Db \subseteq D_n$ , so  $r \neq 0$ . Then  $\delta(b) > \delta(r) \geq n \Rightarrow \delta(b) \geq n + 1 \Rightarrow b \in D_{n+1}$ .

(b) Given  $d \in D \setminus \{0\}$ , define  $\delta(d) := \sup\{n \in \mathbb{N} : d \in D_n\}$ . Then  $\delta : D \setminus \{0\} \rightarrow \mathbb{N}$  is well-defined. Let  $a, b \in D, b \neq 0$ . If  $a + Db \subseteq D_{\delta(b)}$ , then  $b \in D_{\delta(b)+1}$ , i.e.,  $\delta(b) \geq \delta(b) + 1 (\Rightarrow \Leftarrow)$ . Conclude that  $\exists q \in D$  such that either  $a - bq \notin D_{\delta(b)}$ . Let  $r = a - bq$ . Then  $a = bq + r$ , and  $r = 0$  or  $\delta(r) < \delta(b)$ .  $\square$

19. Let  $R$  be an integral domain,  $N : R \setminus \{0\} \rightarrow \{n > 0 : n \in \mathbb{Z}\}$  a function for which (i)  $N(1) = 1$  and (ii)  $N(xy) = N(x)N(y)$  for all  $x, y \in R \setminus \{0\}$ . (a) Let  $K$  be the field of fractions of  $R$ . Show that  $N$  can be extended in a unique way to a function from  $K \setminus \{0\}$  into  $\mathbb{Q}$  that still satisfies (i) and (ii). (b) Show that  $R$  is a Euclidean domain under  $N$  iff for each  $x \in K \setminus R$  there is an element  $r \in R$  for which  $N(x - r) < 1$ .

*Proof.*

(a) Define  $N : K \setminus \{0\} \rightarrow \mathbb{Q}$  by  $N(ab^{-1}) = N(a)/N(b)$ . Then  $N$  is well-defined: If  $a/b = c/d$ , then  $ad = bc \Rightarrow N(a)N(b) = N(ab) = N(bc) = N(b)N(c) \Rightarrow N(a)/N(b) = N(c)/N(d)$ . Also,  $N$  satisfies properties (i) and (ii). Moreover, if  $N'$  is another such function satisfying the required properties, then  $1 = N'(1/1) = N'(a/a) = N'(a)N'(a^{-1})$ , so  $N'(a^{-1}) = N'(a)^{-1}$ . We conclude  $N' = N$ .

(b) Suppose  $R$  is a Euclidean domain under  $N$ . Let  $x \in K \setminus R$ , and write  $x = a/b$  for some  $a, b \in R$ . There exist  $r, s \in R$  such that  $a = rb + s$  and  $s = 0$  or  $N(s) < N(b)$ . Since  $x \notin R$ ,  $s \neq 0$ . Then  $N(s) = N(a - rb) < N(b) \Rightarrow N(x - r) = N(a - rb)N(b)^{-1} < N(b)N(b)^{-1} = N(1) = 1$ . Conversely, suppose that for each  $x \in K \setminus R$ ,  $\exists r \in R$  such that  $N(x - r) < 1$ . Let  $a, b \in R, b \neq 0$ . Assume  $b \nmid a$  in  $R$ . For some  $r \in R$ , we have  $N(\frac{a}{b} - r) < 1 \Rightarrow N(a - rb) = N(b)N(\frac{a}{b} - r) < N(b)$ . Now  $a = br + (a - br)$ ,  $N(a - br) < N(b)$ . Conclude that  $R$  is a Euclidean domain under  $N$ .  $\square$

## Rings of Fractions

20. Let  $R$  be a commutative ring, and let  $S$  be a multiplicatively closed subset of  $R$  containing 1. Show that the prime ideals of  $S^{-1}R$  are in one-to-one correspondence with the prime ideals of  $R$  not containing any element of  $S$ . Is a similar statement true for maximal ideals?

*Proof.* Let  $P \trianglelefteq R$  be a prime ideal not containing any element of  $S$ . Define  $S^{-1}P := \{\frac{a}{b} : a \in P, b \in S\}$ . If  $\frac{a}{b}, \frac{c}{d} \in S^{-1}P$ , then  $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \in S^{-1}P$  because  $ad + bc \in P$  and  $bd \in S$ . If  $\frac{c}{d} \in S^{-1}R$ , then  $\frac{c}{d} \frac{a}{b} = \frac{ac}{bd} \in S^{-1}P$  because  $ac \in P$  and  $bd \in S$ . So  $S^{-1}P \trianglelefteq S^{-1}R$ . Let  $\frac{a}{b}, \frac{c}{d} \in S^{-1}R$ , and suppose  $\frac{a}{b} \frac{c}{d} = \frac{ac}{bd} \in S^{-1}P$ . Then  $ac \in P \Rightarrow a \in P$  or  $c \in P \Rightarrow \frac{a}{b} \in S^{-1}P$  or  $\frac{c}{d} \in S^{-1}P$ . So  $S^{-1}P$  is a prime ideal. Now let  $J \trianglelefteq S^{-1}R$  be a prime ideal, and let  $\widehat{J} = \iota^{-1}(J)$ , where  $\iota : R \rightarrow S^{-1}R$  is the inclusion  $r \mapsto \frac{r}{1}$ . Then  $\widehat{J}$  is a prime ideal of  $R$  (see the Additional Results section).

Let  $\mathcal{A} = \{P \trianglelefteq R : P \text{ prime}, P \cap S = \emptyset\}$ , and let  $\mathcal{B} = \{J \trianglelefteq S^{-1}R : J \text{ prime}\}$ . Let  $\varphi : \mathcal{A} \rightarrow \mathcal{B}$  be defined by  $\varphi(P) = S^{-1}P$ , and let  $\psi : \mathcal{B} \rightarrow \mathcal{A}$  be defined by  $\psi(J) = \widehat{J}$ . Now  $\psi \circ \varphi = \text{id}_{\mathcal{A}}$ , and  $\varphi \circ \psi = \text{id}_{\mathcal{B}}$ , and the result follows.

Consider the case  $R = \mathbb{Q}[x, y]$ . We have that  $P = (x) \trianglelefteq \mathbb{Q}[x, y]$  is a prime ideal because  $\mathbb{Q}[x, y]/(x) \cong \mathbb{Q}[y]$  is an integral domain but not a field. Let  $S = R \setminus P$ , so  $S$  is multiplicatively closed. As will be proved in the following exercise,  $S^{-1}R$  is a local ring, and thus has a unique maximal ideal. If  $I \trianglelefteq R$  is an ideal satisfying  $I \cap S = \emptyset$ , then  $I \subseteq P = (x)$ . But any proper ideal of  $P$  is not a maximal ideal (because it is properly contained in the proper ideal  $P$ , and  $P$  itself is not maximal). So no such correlation exists in general for maximal ideals.  $\square$

21. Show that  $S^{-1}R$  is a local ring if  $S = R \setminus P$  for some prime ideal  $P$  of  $R$ . In this case we write  $R_P := S^{-1}R$ .

*Proof.* Let  $P \trianglelefteq R$  be a prime ideal,  $S = R \setminus P$ . Note that the set of non-units in  $S^{-1}R$  is the set  $I = \{\frac{a}{b} : a \in P, b \in S\}$ . To prove that  $S^{-1}R$  is a local ring, it suffices to prove that  $I \trianglelefteq S^{-1}R$ . If  $\frac{a}{b}, \frac{c}{d} \in I$ , then  $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \in I$  because  $ad+bc \in P$ . If  $\frac{r}{s} \in S^{-1}R$ , then  $\frac{r}{s} \frac{a}{b} = \frac{ra}{sb} \in I$  because  $ra \in P$ . Then  $I \trianglelefteq S^{-1}R$ , so  $S^{-1}R$  is a local ring.  $\square$

22. Prove that  $R$  does not have any nonzero nilpotent elements iff, for all prime ideals  $P \trianglelefteq R$ ,  $R_P$  does not have any nilpotent elements.

*Proof.* Suppose  $r \in R \setminus \{0\}$  is nilpotent. Say  $r^n = 0$ . Let  $I = \text{Ann}_R(r)$ . Now  $I$  is a nonzero proper ideal of  $R$ , hence contained in some maximal (hence prime) ideal  $M$ . Consider the local ring  $R_M$ . We have  $\frac{r}{1} \neq \frac{0}{1}$  in  $R_M$  because  $tr \neq 0$  for all  $t \in R \setminus M$ . But  $(\frac{r}{1})^n = \frac{0}{1}$ . So  $R_M$  has a nonzero nilpotent element. Conversely, let  $P \trianglelefteq R$  be a prime ideal and suppose  $R_P$  has a nonzero nilpotent element  $\frac{r}{s}$  with  $(\frac{r}{s})^n = \frac{0}{1}$ . Then also  $\frac{s}{1} \frac{r}{s} = \frac{r}{1}$  is nilpotent. Now  $tr^n = 0$  for some  $t \in R \setminus P$ , but  $tr \neq 0$ . Then  $tr \in R$  is a nonzero nilpotent element of  $R$ .  $\square$

23. Suppose  $S = \{a^n : n \in \mathbb{N}\}$  ( $a^0 := 1$ ) for some  $a \in R \setminus \{0\}$ . Show  $S^{-1}R \cong R[x]/(ax - 1)$ . What does this mean for nilpotent  $a$ ?

*Proof.* Let  $I = (ax - 1) \trianglelefteq R[x]$ . If  $a$  is nilpotent then  $ax - 1$  is a unit in  $R[x]$ , so  $R[x]/I \cong \{0\} \cong S^{-1}R$ . Assume that  $a$  is not nilpotent. We have the embedding  $\iota : R \rightarrow R[x]$ , and the (not necessarily injective) inclusion  $\varphi : R \rightarrow S^{-1}R$ . Then by the universal property of polynomial rings, we have a unique ring homomorphism  $\phi : R[x] \rightarrow S^{-1}R$  such that  $\phi \circ \iota = \varphi$  and  $\phi(x) = \frac{1}{a}$ . Since  $I \subseteq \ker \phi$ , we are entitled to a ring homomorphism  $\phi : R[x]/I \rightarrow S^{-1}R$  satisfying the same properties as for the original  $\phi$ . Observe that in  $R[x]/I$ ,  $ax + I = ax - (ax - 1) + I = 1 + I$ , so  $(a + I) = (x + I)^{-1}$ . Since we have the (not necessarily injective) ring homomorphism  $\alpha : R \rightarrow R[x]/I$  given by  $r \mapsto r + I$ , by the universal property of rings of fractions we have a ring homomorphism  $\psi : S^{-1}R \rightarrow R[x]/I$  such that  $\psi \circ \varphi = \alpha$ . Evidently,  $\psi(\frac{1}{a}) = x + I$ . One observes that  $\psi \circ \phi = \text{id}_{R[x]/I}$ , and that  $\phi \circ \psi = \text{id}_{S^{-1}R}$ . Hence  $\phi$  and  $\psi$  are inverse isomorphisms, and  $S^{-1}R \cong R[x]/I$ .  $\square$

## 2.2 PIDs, UFDs and Polynomial Rings

1. [Sep 80 #2] (a) Give three examples of PIDs. (b) Show that the homomorphic image of a PIR (Principal Ideal Ring) is again a PIR. (c) Give an example of a PID with a homomorphic image which is not a PID.

*Proof.* (a) If  $\mathbb{F}$  is a field, then  $\mathbb{Z}, \mathbb{F}, \mathbb{F}[x]$  are all PIDs. (b) Let  $R$  be a PIR,  $\phi : R \rightarrow S$  a surjective ring homomorphism. Let  $J \trianglelefteq S$ . Then  $I := \phi^{-1}(J) \trianglelefteq R$ , so  $\exists r \in R$  such that  $I = (r)$ . Then  $J = (\phi(r))$ . (c) The homomorphism  $\mathbb{Z} \rightarrow \mathbb{Z}_6$  reduction mod 6 maps the PID  $\mathbb{Z}$  to a ring which is not a domain (hence not a PID).  $\square$

2. [Aug 88 #1] If  $F$  is a field, prove  $F[x]$  is a PID.

*Proof.* Let  $I \trianglelefteq F[x]$ , and let  $f \in I$  be a nonzero polynomial of minimal degree. Let  $g \in I$ . By the division algorithm, there exist  $q, r \in F[x]$  such that  $g = fq + r$  and  $r = 0$  or  $\deg(r) < \deg(f)$ . If  $r = 0$ , then  $g \in (f) \trianglelefteq F[x]$ . If  $r \neq 0$ , then  $r = g - fq \in I (\Rightarrow \Leftarrow)$ , because  $f \in I$  was chosen to have minimal degree. Conclude that  $r = 0$  and  $I = (f)$ .  $\square$

3. [Jan 81 #4] Show  $F[x]$  is a Euclidean domain, but  $F[x, y]$  is not.

*Proof.* Note that  $F[x]$  is a domain because  $F$  is a domain. Define  $\delta : F[x] \setminus \{0\} \rightarrow \mathbb{N}$  by  $\delta(f) = \deg(f)$ . Then by the division algorithm,  $\delta$  is a Euclidean norm function on  $F[x]$ , and hence  $F[x]$  is a Euclidean domain. Recall that Euclidean  $\Rightarrow$  PID, so to prove  $F[x, y]$  is not Euclidean, it suffices to show that it is not a PID. Consider the ideal  $(x, y) \trianglelefteq F[x, y]$ ,  $(x, y) \neq F[x, y]$ . Suppose  $(x, y) = (g)$  for some  $g \in F[x, y]$ . Note that  $F[x, y]/(x) \cong F[y]$ ,  $F[x, y]/(y) \cong F[x]$  are both integral domains but not fields, so  $(x), (y)$  are both prime ideals of  $F[x, y]$ . Hence  $x, y$  are prime elements of  $F$ , and  $g$  is a common divisor of  $x$  and  $y$ . So  $g \in F[x, y]^* = F$ . But then  $(x, y) = (g) = F[x, y] (\Rightarrow \Leftarrow)$ . Conclude that  $(x, y)$  is not principal.  $\square$

4. [Jan 79 #2] (a) Show that any Euclidean domain  $R$  is a PID. (b) Show that any two nonzero elements  $a, b \in R$  have a gcd in  $R$ . (c) Find (systematically)  $m, n \in \mathbb{Z}$  so that  $421m + 1664n = 1$ .

*Proof.* (a) Let  $R$  be a Euclidean domain with degree function  $d$ . Let  $I \trianglelefteq R$ , and let  $a \in I$  be nonzero of minimal degree. Let  $b \in I$ . Suppose  $b \notin (a)$ . Then  $\exists q, r \in R$  such that  $b = aq + r$  and  $d(r) < d(a)$ . Now  $r = b - aq \in I (\Rightarrow \Leftarrow)$ , because  $a$  was chosen to have minimal degree. Conclude  $b \in (a)$ , hence  $(a) = I$ . (b) Let  $a, b \in R$ , and let  $c \in R$  such that  $(a, b) = (c)$ . Now

$c \mid a$  and  $c \mid b$ . Also,  $\exists r, s \in R$  such that  $ar + bs = c$ . Now if  $g \in R$  satisfies  $g \mid a$  and  $g \mid b$ , then  $g \mid ar + bs = c$ . Conclude that  $c = \gcd(a, b)$ . (c) We have

$$\begin{aligned} 1664 &= 3 \cdot 421 + 401 \\ 421 &= 1 \cdot 401 + 20 \\ 401 &= 20 \cdot 20 + 1 \\ 20 &= 1 \cdot 20 + 0 \end{aligned}$$

Then  $1 = 401 - 20(20) = 401 - 20(421 - 401) = 21 \cdot 401 - 20 \cdot 421 = 21 \cdot (1664 - 3 \cdot 421) - 20 \cdot 421 = 21 \cdot 1664 - 83 \cdot 421$ . So  $m = -83, n = 21$ .  $\square$

5. [Jan 89 #6] Prove or disprove: Every UFD is a PID.

*Proof.* False. Let  $F$  be a field. Then  $F$  is a UFD  $\Rightarrow F[x]$  is a UFD by Gauss's Lemma  $\Rightarrow F[x][y] = F[x, y]$  is a UFD by Gauss's Lemma. But as proved above,  $F[x, y]$  is not a PID.  $\square$

6. [May 91 #2b] Prove or disprove:  $R$  Euclidean domain  $\Rightarrow R[x]$  Euclidean domain and/or any two nonzero elements of  $R[x]$  have a gcd in  $R[x]$ .

*Proof.* The ring of integers  $\mathbb{Z}$  is a Euclidean domain, but  $\mathbb{Z}[x]$  is not Euclidean because the ideal  $(2, x)$  is not principal (and all Euclidean domains are PIDs). On the other hand, let  $R$  be a Euclidean domain. Now  $R$  a Euclidean domain  $\Rightarrow R$  a PID  $\Rightarrow R$  a UFD  $\Rightarrow R[x]$  a UFD. And any two nonzero elements in a UFD have a greatest common divisor.  $\square$

7. [Fall 87 #2] Prove or disprove:  $R$  PID  $\Rightarrow R[x]$  is a PID.

*Proof.* The ring of integers  $\mathbb{Z}$  is a PID, but  $\mathbb{Z}[x]$  is not a PID because the ideal  $(2, x)$  is not principal. On the other hand, if  $R[x]$  is a PID, then  $R$  is a domain. Moreover,  $R$  is the homomorphic image of  $R[x]$  under the evaluation map  $f(x) \mapsto f(0)$ . Since the homomorphic image of a PID is again a PID, we conclude that  $R[x]$  a PID  $\Rightarrow R$  is a PID.  $\square$

8. [Jan 87 #5] If  $R$  is an integral domain, what are necessary and sufficient conditions that  $R[x]$  be: (0) a domain, (1) a PID, (2) a UFD, (3) noetherian.

*Proof.* (0) Have that  $R$  is a domain  $\iff R[x]$  is a domain. (1) Suppose  $R[x]$  is a PID. The evaluation homomorphism  $f(x) \mapsto f(0)$  establishes the isomorphism  $R[x]/(x) \cong R$ , and we conclude that  $(x)$  is a prime ideal of  $R[x]$  because  $R$  is an integral domain, and hence that  $x \in R[x]$  is prime. Prime elements are automatically irreducible, and the principal ideal generated by an irreducible element is maximal among principal ideals. Then  $(x) \trianglelefteq R[x]$

is maximal, which implies that  $R \cong R[x]/(x)$  must be a field. Conversely, if  $R$  is a field, then  $R[x]$  is a PID. (2)  $R$  is a UFD  $\iff R[x]$  is a UFD. One direction follows from Gauss's Lemma, and the other direction follows from some elementary computations. (3) If  $R$  is noetherian, then  $R[x]$  is noetherian by Hilbert's basis theorem. Conversely,  $R$  is the homomorphic image of  $R[x]$  under the map  $f(x) \mapsto f(0)$ , and the homomorphic image of a noetherian ring is noetherian.  $\square$

9. [Jan 83 #3] Let  $R$  be a PID. If  $a, b$  are two nonzero elements in  $R$ , show that they have a lcm.

*Proof.* Let  $c \in R$  such that  $(c) = (a) \cap (b)$ . Then  $a \mid c$  and  $b \mid c$ . Moreover, if  $d \in R$  satisfies  $a \mid d$  and  $b \mid d$ , then  $d \in (a) \cap (b) = (c) \Rightarrow c \mid d$ . So  $c = \text{lcm}(a, b)$ .  $\square$

10. [Aug 96 #5] Let  $R$  be a PID. An ideal  $P$  of  $R$  is called primary if whenever  $ab \in P$  and  $a \notin P$ , then  $b^n \in P$  for some  $n \in \mathbb{N}$  depending on  $b$ . Show that  $P \trianglelefteq R$  is primary iff either  $P = 0$  or  $P = (p^m)$  for some prime  $p \in R$  and some exponent  $m \in \mathbb{N}$ .

*Proof.* Since  $R$  is a domain, the zero ideal is prime. If  $a, b \in R, ab \in \{0\}$  but  $a \notin \{0\}$ , then  $b = 0$ , so  $\{0\}$  is primary (take  $n = 1$ ). If  $P = (p^m)$  for some prime  $p \in P$  and  $m \in \mathbb{N}$ , then if  $ab \in P$ , we have  $p \mid ab$ , so  $p \mid a$  or  $p \mid b$ . Assume  $p \nmid a$ . Then  $b^m \in P$ . Conversely, let  $0 \neq P \trianglelefteq R, P \neq R$  be primary. Say  $P = (c)$ . We can write  $c = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$  for some distinct primes  $p_i \in R$  and exponents  $e_i \in \mathbb{N}$ . Suppose  $n > 1$ . Then  $(p_1^{e_1} p_2^{e_2} \cdots p_{n-1}^{e_{n-1}}) p_n^{e_n} \in P$ , but  $a := p_1^{e_1} p_2^{e_2} \cdots p_{n-1}^{e_{n-1}} \notin P$  because  $c \nmid a$ . But  $(p_n^{e_n})^m \notin P$  for all  $m \in \mathbb{N}$  because  $c \nmid (p_n^{e_n})^m$ . Conclude that  $n = 1$ , and  $P = (p_1^{e_1})$ .  $\square$

11. [Aug 03 #2] Let  $D$  be a PID with field of fractions  $F$ . Show that every element  $x \in F$  can be written as a sum of primary fractions (i.e., with denominators powers of primes):  $x = \sum_{i=1}^n \frac{a_i}{p_i^{e_i}}$  for some  $a_1, \dots, a_n \in D$  and distinct primes  $p_1, \dots, p_n \in D$ .

*Proof.* Let  $x \in D$ . If  $x = 0$ , then write  $x = \frac{0}{p}$  for some prime  $p \in D$ . Otherwise, write  $x = \frac{a}{b}$  for some  $a, b \in D$ . Assume  $(a, b) = (1)$  (or else cancel out any common prime factors of  $a$  and  $b$ ). If  $x \in D^*$ , write  $x = \frac{p}{p}$  for some prime  $p \in D$ . Otherwise, suppose  $p^e \mid b, p^{e+1} \nmid b$  for some prime  $p \in D, e \geq 1$ . Write  $b = p^e m$ . Then  $(p^e m, a) = (1)$ , so  $\exists r_1, r_2 \in D$  such that  $r_1 p^e a + r_2 m = a$ . Then  $x = \frac{r_1 a}{m} + \frac{r_2}{p^e}$ . Now argue by induction on the number of distinct primes in a prime factorization of  $b$ .  $\square$

12. [Aug 01 #4] If  $a$  is an element of a PID  $R$ , show that the left  $R$ -module  $R/Ra$  is simple iff  $a$  is irreducible.

*Proof.* Easy.  $\square$

13. [Aug 95 #4] Show that  $R := \mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} : a, b \in \mathbb{Z}\}$  is not a UFD. (Hint: Show that  $n^2 - 10m^2 \neq \pm 2, 3$  for all  $n, m \in \mathbb{Z}$ . Then argue that  $2, 3$  and  $4 \pm \sqrt{10}$  are not primes in  $\mathbb{Z}[\sqrt{10}]$ .

*Proof.* Note that  $N : R \rightarrow \mathbb{Z}$  defined by  $N(a + b\sqrt{10}) = a^2 - 10b^2$  is multiplicative. So if  $x, y \in R$ , then  $x \mid y \Rightarrow N(x) \mid N(y)$ . Recall that  $R^* = \{x \in R : N(x) = \pm 1\}$ . Note  $N(2) = 4, N(3) = 9, N(4 \pm \sqrt{10}) = 6$ . If  $N(n + m\sqrt{10}) = n^2 - 10m^2 = 2$ , then  $n^2 \equiv 2 \pmod{5}$ . Similarly, if  $N(n + m\sqrt{10}) = 3$ , then  $n^2 \equiv 3 \pmod{5}$ . Note  $2 \equiv -3 \pmod{5}, 3 \equiv -2 \pmod{5}$ . Now  $1^2 \equiv 1 \pmod{5}, 2^2 \equiv 4 \pmod{5}, 3^2 \equiv 4 \pmod{5}, 4^2 \equiv 1 \pmod{5}$ . Conclude that  $n^2$  is not equivalent to any of  $\pm 2, \pm 3 \pmod{5}$  for any  $n \in \mathbb{Z}$ . Then if  $y \in \{2, 3, 4 \pm \sqrt{10}\}$ ,  $y$  can have no proper factorization in  $R$ . (Any such factorization of  $y$  would result in a nontrivial factorization of  $N(y)$  into norms which cannot be realized in  $R$ .) Conclude that if  $y \in \{2, 3, 4 \pm \sqrt{10}\}$ ,  $y$  is irreducible. Clearly  $2 \nmid 4 \pm \sqrt{10}$  in  $R$ , but  $2 \cdot 3 = 6 = (4 + \sqrt{10})(4 - \sqrt{10})$ . Then  $2$  is irreducible but not prime, so  $R$  is not a UFD (because irreducibles are always prime in a UFD).  $\square$

14. [Aug 04 #3] Consider the ring  $R = \mathbb{Z}[\sqrt{-7}] = \{m + n\sqrt{-7} : m, n \in \mathbb{Z}\}$ . (a) Is  $R$  a UFD? Give arguments for your answer. (b) Exhibit an ideal  $I$  in  $R$  which is not principal. Show that your  $I$  is not principal.

*Proof.*

(a) Note that  $R$  is a subring of  $\mathbb{C}$ . Consider the norm function  $N : R \rightarrow \mathbb{N}$  given by  $N(a + b\sqrt{-7}) = a^2 + 7b^2$ , i.e., the absolute value function  $|\cdot|$  on  $\mathbb{C}$  restricted to  $R$ . Then  $N$  is multiplicative. Note also, given  $x = a + b\sqrt{-7} \in R$ ,  $N(x) = 1$  or  $N(x) \geq 4$ . Together these restrictions imply that  $R^* = \{\pm 1\}$  (because  $x \in R^* \Rightarrow N(x) \in \mathbb{Z}^* \Rightarrow N(x) = 1 \Rightarrow x = \pm 1$ ). We have that  $2 \cdot 4 = 8 = (1 + \sqrt{-7})(1 - \sqrt{-7})$ . Since  $N(2) = 4$ , we conclude that the only possible divisors of  $2$  in  $R$  are  $\pm 1, \pm 2$ , i.e., that  $2$  is irreducible in  $R$ . Note  $N(1 + \sqrt{-7}) = N(1 - \sqrt{-7}) = 8$ . Suppose  $ab = 1 + \sqrt{-7}$  is a nontrivial factorization of  $1 + \sqrt{-7}$  (i.e., neither  $a$  nor  $b$  is a unit in  $R$ ). Then  $1 < N(a), N(b) < 8$ , which implies that one of  $N(a), N(b)$  must be equal to  $2$ , and the other equal to  $4$ . But as mentioned above, no element of  $R$  can have norm  $2$ . Conclude that  $1 + \sqrt{-7}, 1 - \sqrt{-7}$  are also irreducible elements of  $R$ . So  $2 \mid (1 + \sqrt{-7})(1 - \sqrt{-7})$  but  $2 \nmid 1 + \sqrt{-7}$  and  $2 \nmid 1 - \sqrt{-7}$  (because  $2$  is not associate to either of  $1 + \sqrt{-7}, 1 - \sqrt{-7}$ ). Then  $2$  is an irreducible which is not a prime, which implies that  $R$  is not a UFD (because irreducibles are always prime in a UFD).

(b) Consider the ideal  $I = (2, 1 + \sqrt{-7}) \trianglelefteq R$ . Suppose  $I$  is a principal ideal. Recall that  $(2)$  is maximal among the principal ideals of  $R$  because  $2$  is irreducible. But  $1 + \sqrt{-7} \notin (2)$ ,

so we must have  $R = I$ . Then  $\exists a, b, c, d \in \mathbb{Z}$  such that

$$1 = (a + b\sqrt{-7}) \cdot 2 + (c + d\sqrt{-7}) \cdot (1 + \sqrt{-7})$$

Then  $1 + 0\sqrt{-7} = (2a + c - 7d) + (2b + c + d)\sqrt{-7}$ . Observe that  $2a + c - 7d \equiv 2b + c + d \pmod{2}$ , but 1 is not congruent to 0 mod 2, ( $\Rightarrow \Leftarrow$ ). Conclude that  $I$  is not principal.  $\square$

15. [Jan 92 #2] Show that a polynomial of degree  $n$  over  $F$  has at most  $n$  roots in  $F$ .

*Proof.* Let  $f \in F[x]$ . Argue by induction on  $n := \deg(f)$ . The result is clear for  $n = 1$ , so assume  $n > 1$ . Suppose  $f$  has a root  $a \in F$ . Then by the division algorithm,  $\exists q, r \in F[x]$  such that  $f(x) = (x - a)q(x) + r(x)$  and either  $r(x) = 0$  or  $\deg(r(x)) < 1 \Rightarrow r(x) \in F$ . Now  $0 = f(a) = (a - a)q(a) + r(a) = r(a)$ . So  $f(x) = (x - a)q(x)$  for some  $q \in F[x]$ . Have that  $q(x) \in F[x]$  is of degree  $n - 1$ , so by the induction hypothesis,  $q(x)$  has at most  $n - 1$  roots in  $F$ . If  $b \neq a$  is another root of  $f$ , we have  $0 = f(b) = (b - a)q(b)$ , so necessarily  $q(b) = 0$ . Conclude that  $f$  has at most  $n$  roots in  $F$ .  $\square$

16. [Jan 97 #4] Give counterexamples of the following statements, with details. Then correct each statement by modifying the specified text. (a) If  $R$  is a *commutative ring*, then a polynomial in  $R[x]$  of degree  $n$  has at most  $n$  roots in  $R$ . (b) If  $R$  is a *division ring*, then a polynomial in  $R[x]$  of degree  $n$  has at most  $n$  roots in  $R$ . (c) If  $R$  is a *unique factorization domain*, then the greatest common divisor  $d$  of two numbers  $a, b \in R$  can be written as  $d = ax + by$  for some  $x, y \in R$ .

*Proof.* (a) Commutative ring  $\rightarrow$  integral domain. The polynomial  $2x^2 + 2 \in \mathbb{Z}_{10}[x]$  has roots 2, 3, 7, 8 in  $\mathbb{Z}_{10}$ . (b) Division ring  $\rightarrow$  integral domain. The polynomial  $x^4 - 1 \in H[x]$  has roots  $\pm 1, \pm i, \pm j, \pm k$ . (c) UFD  $\rightarrow$  PID. In  $\mathbb{Z}[x]$ ,  $\gcd(2, x) = 1$ , but  $2s + xt = 1$  implies that twice the constant term of  $s$  is equal to 1, i.e., that  $2 \in \mathbb{Z}^*$  ( $\Rightarrow \Leftarrow$ ).  $\square$

17. [Apr 77 #4] (a) If  $M \trianglelefteq R$  is a maximal ideal, show  $R/M$  is a field. (b) If  $R$  is a Euclidean domain, show every ideal generated by an irreducible element is maximal.

*Proof.* See §2.1 #17.  $\square$

18. [Sep 79 #7b] Give an example of a prime ideal in  $R$  which is not maximal. Is there an example where  $R$  is a UFD?

*Proof.* Let  $R = \mathbb{Q}[x, y]$ . Then  $R$  is a UFD because  $\mathbb{Q}$  is a UFD. Now  $\mathbb{Q}[x, y]/(x) \cong \mathbb{Q}[y]$  is an integral domain but not a field, so  $(x) \trianglelefteq \mathbb{Q}[x, y]$  is prime but not maximal.  $\square$

19. [Jan 95 #6] Prove that any proper homomorphic image of a PID that remains an integral domain must actually be a field.

*Proof.* Let  $R$  be a PID, and let  $\varphi : R \rightarrow S$  be a ring homomorphism. Let  $I = \ker \varphi$ , and assume  $I \neq R$ . Then  $R/I \cong \varphi(R)$  is an integral domain, so  $I \trianglelefteq R$  is a prime ideal. Say  $I = (p)$  for some prime  $p \in R$ . Prime elements are always irreducible, and the principal ideal generated by an irreducible element is maximal among principal ideals. Conclude that  $I$  is maximal, hence  $\varphi(R) \cong R/I$  is a field.  $\square$

20. [May 90 #4] If  $P$  is a nonzero prime ideal in a UFD, show  $P$  is minimal among nonzero prime ideals iff  $P$  is principal.

*Proof.* Let  $P \trianglelefteq R$  be a nonzero prime ideal which is minimal among nonzero prime ideals. Let  $x \in P, x \neq 0$ . Write  $x$  as a product of primes in  $R$ ,  $x = p_1 p_2 \cdots p_n$ . Now  $p_1 \in P$  or  $p_2 \cdots p_n \in P$ . By induction, we have  $p \in P$  for some prime  $p \in R$ . Then  $0 \neq (p) \subseteq P \rightarrow P = (p)$ . Conversely, let  $P$  be a nonzero prime ideal, and say  $P = (p)$ . Then necessarily  $p \in R$  is prime. Suppose  $0 \neq I \trianglelefteq R$  is a nonzero prime ideal with  $I \subseteq (p)$ . Let  $x \in I \setminus \{0\}$ . We can write  $x = ap^i$  for some  $a \in R, i \geq 1, p \nmid a$ . Now either  $a \in I$  or  $p^i \in I$ . But  $a \in I \Rightarrow a \in P (\Rightarrow \Leftarrow)$  because  $p \nmid a$ . So  $p^i \in I \Rightarrow p \in I \Rightarrow (p) \subseteq I \subseteq (p)$ . Conclude  $I = (p)$ , hence  $(p)$  is minimal among nonzero prime ideals.  $\square$

21. [Aug 98 #5] The Krull dimension of a commutative ring  $R$  is the longest chain of prime ideals properly contained in  $R$ , i.e., the largest integer  $n$  such that there exists a chain  $P_0 < P_1 < \cdots < P_n < R$  ( $P_0 = 0$  allowed if prime) of prime ideals  $P_i$  in  $R$ . If  $R$  is a PID, find its Krull dimension.

*Proof.* If  $R$  is a field, then  $\{0\}$  is the only prime ideal of  $R$ , so  $n = 0$ . Suppose  $R$  is not a field. Then  $R$  contains some nonzero prime element  $p \in R$ , hence contains at least one nonzero prime ideal. Now, by the previous exercise any nonzero prime ideal  $P = (p)$  of  $R$  is minimal among nonzero prime ideals. (Recall PID  $\Rightarrow$  UFD.) Since necessarily  $p \in R$  is prime hence irreducible,  $P$  is maximal among proper ideals of  $R$ . Conclude that  $n = 1$ .  $\square$

22. [Sep 83 #7] If  $R \subseteq S$  are PIDs with  $d = \gcd_R(a, b)$ , show  $d = \gcd_S(a, b)$ .

*Proof.* Have  $(d) = (a, b)$ , so  $\exists r, s \in R$  such that  $d = ra + bs$ . This equality also holds in  $S$ , so if  $d' \mid a$  and  $d' \mid b$  in  $S$ , then necessarily  $d' \mid ra + bs = d$ . Conclude  $d = \gcd_S(a, b)$ .  $\square$

23. [Mar 83 #5] If  $D$  is a UFD whose units together with 0 form a proper subring  $U$ , show  $D$  has infinitely many (nonassociate) primes. Give an example of such a  $D$ .

*Proof.* Suppose  $D$  has only finitely many nonassociate primes  $p_1, \dots, p_n$ . Let  $p = p_1 \cdots p_n + 1$ . If  $p \in D^*$ , then  $p - 1 = p_1 \cdots p_n \in D^*$  ( $\Rightarrow \Leftarrow$ ). But  $p_i \nmid p$  for all  $1 \leq i \leq n$  ( $\Rightarrow \Leftarrow$ ). Conclude that  $D$  must have infinitely many nonassociate primes. The units of the ring  $\mathbb{Q}[x]$  together with zero form a proper subring  $\mathbb{Q}$ .  $\square$

24. [Sep 82 #2] If  $a_1, \dots, a_n$  in a PID  $R$  have gcd  $d$ , show that there exists an invertible  $n \times n$  matrix  $Q$  of determinant 1 over  $R$  with  $Q[a_1, \dots, a_n]^T = [d, 0, \dots, 0]^T$ . (This is false if  $R$  is merely a UFD.)

*Proof.*  $\square$

25. [Aug 89 #4] Show  $R = \{f(x) \in \mathbb{Z}[x] : \text{the coefficient of } x \text{ in } f(x) \text{ is even}\}$  is a subring of  $\mathbb{Z}[x]$ . Show that 2 and  $2x$  have a gcd in  $R$ , but not a lcm.

*Proof.* The only divisors of 2 in  $\mathbb{Z}[x]$  are 1 and 2. But  $2 \nmid 2x$  in  $R$ , so  $\gcd_R(2, 2x) = 1$ . Suppose 2,  $2x$  have a lcm, say  $m = \text{lcm}_R(2, 2x)$ . Then  $m \nmid 4x = 2 \cdot 2x \Rightarrow m = 4x$  because  $2x$  is not a multiple of 2 in  $R$ . Now  $2 \mid 4x(x+1) = 2 \cdot (2x^2 + 2x)$ ,  $2x \mid 4x(x+1) = 2x(2x+1)$ , but  $4x \nmid 4x(x+1)$  in  $R$  ( $\Rightarrow \Leftarrow$ ). Conclude that 2,  $2x$  do not have a lcm in  $R$ .  $\square$

26. Prove that the ideal  $(x^2 + 2, x^2 + 7)$  is maximal in  $\mathbb{Z}[x]$ .

*Proof.* It suffices to show that  $\mathbb{Z}[x]/(x^2 + 2, x^2 + 7)$  is a field. Let  $I = (x^2 + 2, x^2 + 7)$ . By the Division Algorithm, every coset  $g + I$  has a representative of degree  $\leq 1$ . Since  $5 = (x^2 + 7) - (x^2 + 2) \in I$ , every coset  $g + I$  has a representative of the form  $g = ax + b$  with  $0 \leq a, b \leq 4$ . Now

$$\begin{aligned} (2 + I)^{-1} &= (3 + I) \\ (4 + I)^{-1} &= (4 + I) \\ (x + I)(2x + I) &= 2x^2 + I = 2x^2 - 2(x^2 + 7) + I = -14 + I = 1 + I \\ (x + 1 + I)(x + 3 + I) &= (x + 1 + I)(x - 2 + I) = (x + 1 + I)(x^2 + x + I) \\ &= x(x^2 + 2x + 2) + I = (x + I)(2x + I) = 1 + I \\ (x + 2 + I)(x + 4 + I)(x + 3 + I) &= (x^2 + 6x + 8 + I)(x + 3 + I) \\ &= (x + 1 + I)(x + 3 + I) = 1 + I \end{aligned}$$

So given  $0 \leq a, b \leq 4$ ,  $a, b$  not both zero, have  $(a^{-1} + I)(ax + b + I)$  is of one of the forms above, each of which is invertible. Conclude that  $\mathbb{Z}[x]/I$  is a field, hence  $I$  is maximal.  $\square$

27. [Aug 94 #3] Describe which polynomials in  $\mathbb{R}[x]$  belong to the subring  $\mathbb{R}[x^2, x^3]$ ,  $\mathbb{R}$  the field of real numbers.

*Proof.* We have  $x^2, x^3, (x^2)^2 = x^4, (x^2x^3) = x^5 \in \mathbb{R}[x^2, x^3]$ . Given  $x^{n-2}, x^{n-1}, x^n \in \mathbb{R}[x^2, x^3]$ , we have  $x^{n-2}x^3 = x^{n+1} \in \mathbb{R}[x^2, x^3]$ . Let  $S = \{f(x) \in \mathbb{R}[x] : \text{coefficient of } x \text{ equals zero}\}$ . Then  $S \subseteq \mathbb{R}[x^2, x^3]$ . If  $f = \sum_{i=0}^n a_i x^i, g = \sum_{j=0}^m b_j x^j \in \mathfrak{S}$ , then the coefficient of  $x$  in  $fg$  is  $a_0 b_1 + a_1 b_0 = a_0 \cdot 0 + 0 \cdot b_0 = 0$ , so  $fg \in S$ . Now  $S$  is a ring containing  $\mathbb{R}, x^2, x^3$ , and  $S \subseteq \mathbb{R}[x^2, x^3]$ , so we conclude  $S = \mathbb{R}[x^2, x^3]$ .  $\square$

28. [Feb 84 #5] Factor  $x^3 - y^3$  into irreducible factors in  $\mathbb{Q}[x, y]$ .

*Proof.* Observe  $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$ . Let  $f(x, y) = x^2 + xy + y^2$ . Consider  $g(x) := x^2 + xy + y^2 \in \mathbb{Q}[y][x]$ . Have that  $f$  is irreducible in  $\mathbb{Q}[x, y]$  iff  $g$  is irreducible in  $\mathbb{Q}[y][x]$ . If  $g$  factors in  $\mathbb{Q}[y][x]$ , it must factor into a product of linear polynomials,  $g(x) = (x - \frac{y}{2}(-1 + i))(x - \frac{y}{2}(-1 - i))$ . But  $\frac{y}{2}(-1 + i) \notin \mathbb{Q}[x]$ . Conclude  $g(x)$  is irreducible in  $\mathbb{Q}[y][x]$ , hence  $f(x, y)$  is irreducible in  $\mathbb{Q}[x, y]$ .  $\square$

29. [Jan 94 #3] Prove that  $f(x, y) = y^3 + x^2 y^2 + x^3 y + x$  is irreducible in  $\mathbb{Z}[x, y]$ .

*Proof.* Have that  $f$  is Eisenstein at  $p = x$  in  $\mathbb{Z}[x][y]$ , hence  $f$  is irreducible in  $\mathbb{Z}[x][y] = \mathbb{Z}[x, y]$ .  $\square$

30. [1985 #3a] Show  $f(x) = x^5 - 6x^3 + 12x^2 + 21x - 3$  is irreducible in  $\mathbb{Q}[x]$ .

*Proof.* Have that  $f$  is Eisenstein at  $p = 3$  in  $\mathbb{Z}[x]$ , so  $f$  is irreducible in  $\mathbb{Z}[x]$ . Then  $f$  is irreducible in  $\mathbb{Q}[x]$  by Gauss's Lemma.  $\square$

31. [Aug 96 #4] In  $\mathbb{Q}[x]$ , let  $f(x) = x^{m_1} + \cdots + x^{m_k}$  where  $m_i \equiv i - 1 \pmod{k}$ . Show that  $f(x)$  is divisible by  $x^{k-1} + x^{k-2} + \cdots + 1$ .

*Proof.* Observe that  $x^k - 1 = (x - 1)(x^{k-1} + x^{k-2} + \cdots + x + 1)$ , where the latter of the two factors is the product of all distinct irreducible polynomials over  $\mathbb{Q}$  of primitive  $n$ -th roots of unity for  $n \mid k$ . Let  $\zeta \in \mathbb{C}$  be a primitive  $n$ -th root of unity for  $n \mid k$ . Have  $f(\zeta) = \zeta^{m_1} + \zeta^{m_2} + \cdots + \zeta^{m_k} = 1 + \zeta + \zeta^2 + \cdots + \zeta^{k-1} = 0$  since  $\zeta^k = 1$ . Then  $\zeta$  is a root of  $f$ , so the irreducible polynomial of  $\zeta$  over  $\mathbb{Q}$  must divide  $f$ . This is true for all primitive  $n$ -th roots of unity with  $n \mid k$ , so we conclude  $x^{k-1} + x^{k-2} + \cdots + 1 \mid f(x)$ .  $\square$

32. [Aug 95 #5] Factor  $f(x) = x^9 - x$  in  $\mathbb{F}_3[x]$  into irreducible factors.

*Proof.* Note that  $f$  splits over  $\mathbb{F}_9$ , a field of degree 2 over  $\mathbb{F}_3$ . So the irreducible factors in a factorization of  $f$  can have degree no greater than 2 (otherwise by adjoining a root we'd have a field extension of degree  $> 2$ ). Now  $x^9 - x = x(x^8 - 1) = x(x^4 + 1)(x^4 - 1) = x(x^2 - 1)(x^2 + 1)(x^4 + 1) = x(x - 1)(x - 2)(x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2)$ , where the last two factors are irreducible over  $\mathbb{F}_3[x]$  because they have no roots in  $\mathbb{F}_3$ .  $\square$

33. [Jan 00 #6] Given a finite field  $K$ , show there exists a polynomial  $f(x, y) \in K[x, y]$  (in which both variables actually appear) for which the equation  $f(x, y) = 0$  has no solutions in  $K \times K$ .

*Proof.* Enumerate  $K$  as  $K = \{a_1, \dots, a_n\}$ . Let  $f(x, y) = 1 + (\prod_{i=1}^n (x - a_i)) (\prod_{i=1}^n (y - a_i))$ . Then  $f \neq 0$  ( $f$  has leading term  $x^n y^n$ ) and  $f(m, n) = 1$  for all  $m, n \in K$ .  $\square$

## 2.3 Non-commutative Rings

Here  $R$  is a not necessarily commutative ring with unit 1.

1. [Aug 98 #2] If  $(a + b)^2 = a^2 + b^2$  for all  $a, b \in R$ , show  $R$  is commutative.

*Proof.* Observe that  $1 + 1 = (1 + 1)^2 = (1 + 1)(1 + 1) = 1 + 1 + 1 + 1$ . So  $1 + 1 = 0$ , i.e.,  $1 = -1$ . Then  $a = -a$  for all  $a \in R$ . Now given  $a, b \in R$ , have  $a^2 + b^2 = (a + b)^2 = (a + b)(a + b) = a^2 + ab + ba + b^2 \Rightarrow 0 = ab + ba = ab - ba$ . So  $ab = ba$ .  $\square$

2. [Sep 86 #7] (a) Define the quaternions  $H$  over the reals. (b) Show that any homomorphism of  $H$  into the complex numbers is identically zero. (c) Prove that the equation  $x^2 + 1 = 0$  has infinitely many solutions in  $H$ . Why can't you deduce from the "factorization"  $x^2 + 1 = (x + i)(x - i)$  and the fact that  $H$  is a division ring that there are only two solutions? (d) How many solutions has the equation  $x^2 - 1 = 0$  in  $H$ ?

*Proof.* (a)  $H := \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ . Addition is defined componentwise, and multiplication is extended  $\mathbb{R}$ -linearly from multiplication in  $Q_8$ . (b) Recall that the quaternions form a division ring. (If  $0 \neq x = a + bi + cj + dk$ , then  $x^{-1} = (a - bi - cj - dk)/(a^2 + b^2 + c^2 + d^2)$ .) Let  $f : H \rightarrow \mathbb{C}$  be a ring homomorphism. Then  $\ker f \trianglelefteq H$ , so either  $\ker f = \{0\}$  or  $\ker f = H$ . Now  $f(i^2) = f(j^2) = f(k^2) = f(-1)$ . Note  $f(i^2) = f(i)^2$ ,  $f(j^2) = f(j)^2$ ,  $f(k^2) = f(k)^2$ . Let  $y = \sqrt{f(-1)}$ . By the pigeonhole principle, two of  $f(i)$ ,  $f(j)$ ,  $f(k)$  must equal  $y$ . Say  $f(i) = f(j) = y$ . Then  $i - j \in \ker f \Rightarrow \ker f \neq 0 \Rightarrow f \equiv 0$ . (c) The given "factorization" of  $x^2 + 1$  over  $H$  is false because  $i$  does not commute with all  $x \in H$ . If  $z = bi + cj + dk$  and  $b^2 + c^2 + d^2 = 1$ , then  $z^2 + 1 = 0$ . Since there are infinitely many triples  $(b, c, d)$  satisfying  $b^2 + c^2 + d^2 = 1$ , the equation  $x^2 + 1 = 0$  has infinitely many solutions in  $H$ . (d) We have a true factorization  $x^2 - 1 = (x + 1)(x - 1)$  over  $H$ , so the equation  $x^2 - 1 = 0$  has only two solutions in  $H$  (namely,  $\pm 1$ ).  $\square$

3. [1985 #3d] An element of  $R$  is nilpotent if  $x^n = 0$  for some  $n \in \mathbb{N}$ . Show that if  $x, y$  are commuting nilpotent elements in  $R$ , then  $x + y$  is nilpotent. Give an example to show this is not true if  $x, y$  do not commute.

*Proof.* Let  $x, y \in R$  be nilpotent with  $x^n = y^m = 0$ . The claim follows after first expanding  $(x + y)^{n+m}$  using the binomial theorem. Consider the elements  $A, B \in M_2(\mathbb{R})$ ,

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

Then  $A, B$  are each nilpotent but  $A + B$  is not nilpotent. □

4. [Sep 84 #2] Let  $L$  be a left ideal in  $R$ . (a) Show  $I(L) := \{a \in R : La \subseteq L\}$  is the largest subring  $S$  of  $R$  such that  $L$  is a two-sided ideal of  $S$ . (b) Prove that  $R$  is a division ring iff  $I(L) = L$  for all nonzero  $L$ .

*Proof.* (a) If  $a, b \in I(L)$ , then  $L(a + b) = La + Lb \subseteq L + L = L$ , and  $L(ab) \subseteq Lb \subseteq L$ , so  $a + b, ab \in I(L)$ , so  $I(L)$  is a subring of  $R$ . If  $S$  is a subring of  $R$  such that  $L$  is a two-sided ideal of  $S$ , then for each  $s \in S$ ,  $Ls \subseteq L$ , and we conclude  $S \subseteq I(L)$ . (b) If  $R$  is a division ring, then the only nonzero ideal of  $R$  is  $R$  itself, in which case  $I(R) = R$ . Conversely, suppose  $I(L) = L$  for all nonzero left ideals  $L$  of  $R$ . Let  $a \in R \setminus \{0\}$ , and let  $L = (a)$ . Now  $1 \in I(L) = L$ , so  $\exists b \in R$  such that  $ba = 1$ , i.e.,  $a \in R^*$ . Then  $R$  is a division ring. □

5. [Aug 98 #5] A derivation  $D$  of a ring  $R$  is a map of  $R$  into itself such that  $D(a + b) = D(a) + D(b)$  and  $D(ab) = D(a)b + aD(b)$  for all  $a, b \in R$ . Show that if  $D$  is a derivation, and in addition  $D^2 = 0$  and  $R$  has no 2-torsion ( $2a = 0 \Rightarrow a = 0$ ), then the exponential map  $\text{id} + D$  is an automorphism of  $R$ .

*Proof.* □

6. [Nov 77 #10] Let  $F$  be a field of characteristic  $p > 0$ . A  $p$ -polynomial is a polynomial  $f(x) = \sum_{i=0}^n a_i x^{p^i}$ . If  $a_n \neq 0$ , then  $f$  has degree  $n$ . (a) Show that the set  $R$  of all  $p$ -polynomials becomes a non-commutative ring under the usual addition and the substitution product  $f(x) * g(x) := f(g(x))$ . Does  $R$  have a unit element? What are the zero divisors? (b) Show that every left ideal  $I$  in  $R$  is principal,  $I = Rf$  for some  $f \in I$ . (c) Show that every right ideal of  $R$  is principal iff the field  $F$  is perfect ( $F^p = F$ ). (d) Are there any perfect fields  $F$  for which  $R$  is commutative?

*Proof.*

(a) The ring  $R$  is certainly an additive abelian group. Associativity of multiplication follows from the associativity of functional composition. In particular, given any  $g(x) \in F[x]$ , there exists an  $F$ -linear homomorphism  $H : F[x] \rightarrow F[x]$  satisfying  $x \mapsto g(x)$ . Associativity of the substitution product follows from composing an

appropriate sequence of such homomorphisms. Appealing to such homomorphisms also establishes the right distributive law:  $(f + g) * h = f * h + g * h$ . Recall that in characteristic  $p$ ,  $(a + b)^{p^n} = a^{p^n} + b^{p^n}$  for all  $n \geq 0$ . The left distributive law  $f * (g + h) = f * g + f * h$  now follows. Note that  $x * f = f = f * x$  for all  $f \in R$ . Also, if  $f = \sum_{i=0}^n a_i x^{p^i}$ ,  $g = \sum_{j=0}^m b_j x^{p^j}$ , then the highest power term of  $f * g$  is  $a_n (b_m x^{p^m})^{p^n} = (a_n b_m^{p^n}) x^{p^{n+m}}$ . Conclude that  $\deg(fg) = \deg(f) + \deg(g)$ , and  $R$  has no nonzero zero divisors. Thus  $R$  is a ring with unit  $1_R = x$ .

- (b) Let  $I$  be a left ideal of  $R$ . Let  $f \in I$  be of minimal degree. Assume that the leading coefficient  $a$  of  $f$  is 1 (or else consider  $f' = a^{-1}x * f$ , a polynomial of leading coefficient 1 and  $\deg(f') = \deg(f)$ ). Suppose  $I \neq Rf$ . Let  $g \in I \setminus Rf$  be of minimal degree. Say  $\deg(f) = n, \deg(g) = m$ . Suppose  $g$  has leading coefficient  $b \in F$ . Then  $g - bx^{p^{m-n}} * f \in I \setminus Rf$  is a polynomial of degree  $< m$  ( $\Rightarrow \Leftarrow$ ). Conclude that  $I = Rf$ .
- (c) Assume that the field  $F$  is perfect. Let  $I$  be a right ideal of  $R$ , and let  $f \in R$  be of minimal degree,  $\deg(f) = m$ . Assume that the leading coefficient  $a$  of  $f$  is 1 (or else consider the polynomial  $f' = f * (bx)$ ,  $b^{p^m} = a$ , a monic polynomial of the same degree as  $f$ ). (Such a  $b \in F$  exists because  $F$  is perfect.) Suppose  $I \neq fR$ . Let  $g \in I \setminus fR$  be of minimal degree. Say  $\deg(g) = m$  and  $g$  has leading coefficient  $c \in F$ . Let  $d \in F$  such that  $d^{p^n} = c$ . Then  $g - f * (dx^{p^{m-n}}) \in I \setminus fR$  has degree  $< m$  ( $\Rightarrow \Leftarrow$ ). Conclude  $I = fR$ . Conversely, assume that every right ideal of  $R$  is principal. Consider the right ideal  $I = (\{ax^p : a \in F\})$ . Say  $I = fR$ . Now  $\deg(f) \neq 0$  because  $x \notin I$ . If  $\deg(f) > 1$ , then  $\deg(g) > 1$  for all  $g \in I$ . Conclude that  $\deg(f) = 1$ . Say  $f = bx^p + cx$ . Then  $c = 0$ , or else  $cx = f - bx^p \in I$  ( $\Rightarrow \Leftarrow$ ), because  $x \notin I$ . Let  $a \in F$ . Then  $\exists d \in F$  such that  $f * dx = bax^p$ , i.e.,  $bd^p x^p = bax^p$ . Then  $d^p = a$ . Then the injective field homomorphism  $\sigma_p : F \rightarrow F^p$  given by  $\sigma_p(a) = a^p$  is also surjective, hence an isomorphism, and  $F = F^p$ , i.e.,  $F$  is perfect.
- (d) Any finite field is perfect. Consider the case  $F = \mathbb{Z}_2$ . Observe that  $x^{p^m} * x^{p^n} = x^{p^{m+n}} = x^{p^n} * x^{p^m}$ . So by induction, the distributive laws and the binomial theorem mod 2,  $R$  is commutative when  $F = \mathbb{Z}_2$ .  $\square$

7. [May 89 #2] Show that in a general ring  $R$  (not necessarily commutative or with unit), all the elements that are not divisors of zero have the same additive order. What are the possible values for this order?

*Proof.* For  $x \in R \setminus \{0\}$ , define  $\text{char}(x) := \inf\{n \in \mathbb{N} : nx = \overbrace{x + \cdots + x}^n = 0\}$ , with  $\text{char}(x) =$

$\infty$  if  $nx \neq 0$  for all  $n \in \mathbb{N}$ . Let  $x, y \in R$ , and suppose  $\text{char}(x) = n < m = \text{char}(y)$ . Then

$$0 = \overbrace{(x + \cdots + x)}^n(y) = \overbrace{xy + \cdots + xy}^n = x \overbrace{(y + \cdots + y)}^n$$

Conclude that  $x$  is a zero divisor because  $ny \neq 0$ . Hence if  $x, y \in R$  are not zero divisors, we must have  $\text{char}(x) = \text{char}(y)$ . Now define  $\text{char}(R) := \text{char}(x)$  for any nonzero element  $x \in R$  which is not a zero divisor. Let  $n \in \mathbb{N}$ , and pick a prime  $p > n$ . Consider the ring  $R = \mathbb{Z}/(pn)\mathbb{Z}$ . Given  $m \in \mathbb{Z}$ , we have  $pn \mid pm \iff n \mid m$ . Conclude that  $p + (pn)\mathbb{Z}$  is an element of additive order  $n$ , because  $m(p + (pn)\mathbb{Z}) = (pm + (pn)\mathbb{Z}) = 0 \Rightarrow n \mid m$ , i.e.,  $m \geq n$ .  $\square$

8. [Jan 94 #5] Give an example of a ring  $R$  without identity and an ideal in the ring direct sum  $R \oplus R$  that does not have the form  $I_1 \oplus I_2$  where the  $I_k$  are ideals in  $R$ .

*Proof.* Let  $R = 2\mathbb{Z}$ , and let  $I$  be the principal ideal generated by  $(2, 4)$ . If  $I = I_1 \oplus I_2$  for some  $I_1, I_2 \trianglelefteq R$ , then  $(2, 0) \in I_1 \Rightarrow (2, 0) \in I \Rightarrow (a, b)(2, 4) = (2, 0)$  for some  $a, b \in 2\mathbb{Z}$ . But  $2a \neq 2$  for all  $a \in 2\mathbb{Z}$ . Conclude that  $I$  does not have the form  $I = I_1 \oplus I_2$ .  $\square$

## 2.4 Additional Results

**Problem.** Let  $R, S$  be commutative rings,  $I \trianglelefteq R, J \trianglelefteq S$ ,  $\varphi : R \rightarrow S$  a ring homomorphism. Prove or disprove:

- (a)  $\varphi(I) \trianglelefteq S$ .
- (b)  $\varphi^{-1}(J) \trianglelefteq R$ .
- (c)  $J$  prime in  $S \Rightarrow \varphi^{-1}(J)$  prime in  $R$ .
- (d)  $J$  maximal in  $S \Rightarrow \varphi^{-1}(J)$  maximal in  $R$ .

Now assume that  $\varphi$  is surjective.

- (e)  $\varphi(I) \trianglelefteq S$ .
- (f) If  $I \neq R$ , then  $\varphi(I) \neq S$ .
- (g)  $I$  prime in  $R$  and  $\varphi(I) \neq S$ , then  $\varphi(I)$  prime in  $S$ .
- (h)  $M$  maximal in  $R$ ,  $\varphi(M) \neq S$ , then  $\varphi(M)$  maximal in  $S$ .
- (i)  $J$  maximal in  $S \Rightarrow \varphi^{-1}(J)$  maximal in  $R$ .

**Solution.**

- (a) False.  $R = \mathbb{Z}$ ,  $S = \mathbb{Z}[x]$ ,  $\varphi$  the inclusion map. Then  $\varphi(\mathbb{Z}) = \mathbb{Z}$  is not an ideal of  $\mathbb{Z}[x]$ .
- (b) True.
- (c) True.
- (d) False.  $R = \mathbb{Z}$ ,  $S = \mathbb{Z}_2$ ,  $\varphi$  the zero homomorphism. Now  $J = \{0\} \trianglelefteq \mathbb{Z}_2$  is maximal, but  $\varphi^{-1}(J) = R$  is not maximal in  $R$ .
- (e) True.
- (f) False.  $R = \mathbb{Z}$ ,  $S = \mathbb{Z}_5$ ,  $I = 2\mathbb{Z}$ ,  $\varphi =$  reduction mod 5. Then  $\varphi(I) = S$ .
- (g) False.  $R = \mathbb{Z}[x]$ ,  $S = \mathbb{Z}$ ,  $I = (x + 1)$ ,  $\varphi$  given by  $f(x) \mapsto f(1)$ . Then  $\varphi(I) = 4\mathbb{Z}$ , which is not prime in  $S$ .
- (h) True.
- (i) True.

**Lemma.** Let  $R$  be a commutative ring,  $a, b \in R$ . Let  $m, n \in \mathbb{N}$  with  $(m, n) = 1$ , and suppose  $a^n = b^n, a^m = b^m$ . Then  $a - b$  is nilpotent.

**Solution.** It suffices to show that  $a - b \in P$  for every prime ideal  $P$  of  $R$ . Observe that the relation  $a^n = b^n$  implies that  $a$  is nilpotent iff  $b$  is nilpotent. If  $a$  (and hence  $b$ ) is nilpotent, then  $a - b$  is nilpotent because  $a$  and  $b$  commute. So assume that  $b$  is not nilpotent. Let  $S = \{b^k : k \geq 0\}$ , with  $b^0 := 1$ . Consider the ring of fractions  $S^{-1}R$ . In  $S^{-1}R$ , we have  $(\frac{a}{b})^n = \frac{1}{1}$  and  $(\frac{a}{b})^m = \frac{1}{1}$ . Conclude that  $\frac{a}{b}$  is a unit in  $S^{-1}R$  of order dividing both  $m$  and  $n$ , i.e.,  $\frac{a}{b} = \frac{1}{1}$ . Then  $(a - b)b^j = 0$  for some  $j \geq 0$ . Assume  $j \geq 1$ . Let  $P \trianglelefteq R$  be a prime ideal. Now  $(a - b)b^j = 0 \in P$ , so either  $a - b \in P$  or  $b^j \in P$ . Now  $b^j \in P \Rightarrow b \in P$ . But then also  $a^n = b^n \in P \Rightarrow a \in P$ . Then  $a - b \in P$ . Conclude that  $a - b \in \bigcap \{P : P \trianglelefteq R \text{ is prime}\} = \text{nilradical}(R)$ , i.e.,  $a - b$  is nilpotent.

**Theorem.** Let  $R$  be a commutative ring with identity having no nonzero nilpotent elements. Then  $R[x]^* = R^*$ .

*Proof.* The inclusion  $R^* \subseteq R[x]^*$  is trivial. Let  $p(x) \in R[x]^*$ , and write  $p(x) = \sum_{k=0}^n a_k x^k$ . Suppose  $\deg(p) > 0$ . We have  $a_0 \in R^*$ , because  $a_0$  is the homomorphic image of  $p$  under the evaluation homomorphism  $p(x) \mapsto p(0)$ , and the homomorphic image of a unit is a unit. Let  $q(x) = p(x)^{-1}$ , and write  $q(x) = \sum_{j=0}^m b_j x^j$ . If  $\deg(q) = 0$ , then  $b_0 a_n = b_0 a_{n-1} = \cdots =$

$b_0a_1 = 0$ , which implies that  $b_0 \in R$  is a zero divisor because  $a_n \neq 0$ . This is a contradiction, because  $q(x)$  was assumed to be a unit. So  $\deg(q) > 0$ . Now we must have  $a_nb_m = 0$ . Consider the coefficient of  $x^{n+m-1}$  in  $p(x)q(x)$ . We have

$$\begin{aligned} 0 &= a_{n-1}b_m + a_nb_{m-1} \Rightarrow \\ 0 &= a_n(a_{n-1}b_m) + a_n(a_nb_{m-1}) \\ &= a_{n-1}(a_nb_m) + a_n^2b_{m-1} \\ &= 0 + a_n^2b_{m-1} = a_n^2b_{m-1} \end{aligned}$$

Now suppose  $a_n^{j+1}b_{m-i} = 0$  for all  $0 \leq i \leq j$ . If  $j+1 < m+n$ , the coefficient of  $x^{m+n-(j+1)}$  must be zero. Then

$$\begin{aligned} 0 &= a_nb_{m-(j+1)} + a_{n-1}b_{m-j} + \cdots + a_{n-(j+1)}b_m \Rightarrow \\ 0 &= a_n^{j+1}(a_nb_{m-(j+1)} + a_{n-1}b_{m-j} + \cdots + a_{n-(j+1)}b_m) \\ &= a_n^{j+2}b_{m-(j+1)} + a_{n-1}(a_n^{j+1}b_{m-j}) + \cdots + a_{n-(j+1)}(a_n^{j+1}b_m) \\ &= a_n^{j+2}b_{m-(j+1)} + 0 = a_n^{j+2}b_{m-(j+1)} \end{aligned}$$

Conclude that  $a_n^{j+1}b_{m-i} = 0$  for  $0 \leq i \leq j$  and  $j+1 < n+m$ . (As usual, we have adopted the convention that  $a_k, b_k = 0$  for  $k < 0$ ,  $a_k = 0$  for  $k > n$ , and  $b_k = 0$  for  $k > m$ .) Now consider the coefficient of  $x^n$  in the product  $p(x)q(x)$ . We have

$$\begin{aligned} 0 &= a_nb_0 + a_{n-1}b_1 + \cdots + a_0b_n \Rightarrow \\ 0 &= a_n^{(m-1)+1}(a_nb_0 + a_{n-1}b_1 + \cdots + a_0b_n) \\ &= a_n^{m+1}b_0 + a_{n-1}(a_n^mb_1) + \cdots + a_0(a_n^mb_n) \\ &= a_n^{m+1}b_0 + 0 = a_n^{m+1}b_0 \end{aligned}$$

Then  $a_n^{m+1} = 0$  and  $a_n$  is nilpotent (because  $b_0 \in R^*$  and hence is not a zero divisor).  $\square$

# Chapter 3

## Modules and Canonical Forms

### 3.1 Modules

1. [Sep 84 #6] Find the invariant factors of the following  $3 \times 3$  matrices over  $\mathbb{Z}$ , and decide if they are equivalent.

$$\begin{pmatrix} 10 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 6 \end{pmatrix} \quad \begin{pmatrix} 4 & 6 & 4 \\ 4 & 20 & 12 \\ 20 & 0 & 20 \end{pmatrix}$$

*Proof.*

□

2. [Aug 97 #7] Let  $M$  be a free module over  $\mathbb{Q}[x]$  with basis  $v_1, v_2, v_3$ ,  $N$  a submodule with basis  $w_1, w_2, w_3$ , where

$$\begin{aligned} w_1 &= (x^3 - x^2 - x + 1)v_1 + (2x^2 + 2x)v_2 + (x^3 + x^2)v_3 \\ w_2 &= (2x^3 - 3x^2 - 3x + 2)v_1 + (5x^2 + 5x)v_2 + (2x^3 + 2x^2)v_3 \\ w_3 &= (x^3 - x)v_1 + (x^2 + x)v_2 + (x^3 + x^2)v_3 \end{aligned}$$

- (a) There is a theorem which implies that  $M$  has another basis  $u_1, u_2, u_3$  for which  $d_1u_1, d_2u_2, d_3u_3$  are a basis for  $N$  for some  $d_1, d_2, d_3 \in \mathbb{Q}[x]$  such that  $d_1 \mid d_2 \mid d_3$ . State the theorem. (b) Find  $d_1, d_2, d_3$ .

*Proof.* (a) Let  $M$  be a finitely generated free module over a PID  $R$ ,  $N$  a submodule of  $M$ . Then there exists an  $R$ -basis  $y_1, \dots, y_n$  of  $M$  ( $n = \text{rk}_R(M)$ ), and nonzero  $d_1, \dots, d_m$  ( $m \leq n$ ) such that  $d_1|d_2|\dots|d_m$  and  $d_1y_1, \dots, d_my_m$  is an  $R$ -basis for  $N$ .

(b) Begin by factoring each polynomial to get the matrix

$$\begin{pmatrix} (x+1)(x^2-2x+1) & (x+1)(2x) & (x+1)(x^2) \\ (x+1)(2x^2-5x+2) & (x+1)(5x) & 2x^2(x+1) \\ (x+1)(x^2-x) & (x+1)x & x^2(x+1) \end{pmatrix}$$

After dropping the term  $(x+1)$  from each entry, use elementary row and column operations to transform the matrix to  $\text{diag}(1, x, x^2)$ . Then  $d_1 = x+1$ ,  $d_2 = x(x+1)$ , and  $d_3 = x^2(x+1)$ .  $\square$

3. [May 91 #6] Let  $M = \mathbb{Z} \oplus \mathbb{Z}$  be the free module of rank 2 over the ring  $\mathbb{Z}$  of integers. Let  $S$  be the submodule of  $M$  spanned by  $x = (3, 0)$ ,  $y = (0, 4)$ ,  $z = (6, 2)$ . Find a  $\mathbb{Z}$ -basis for the submodule  $S$ .

*Proof.* Let  $e_1 = (1, 0)$  and  $e_2 = (0, 1)$ . Use elementary row and column operations to change the matrix whose rows are  $x, y, z$  (reading down) into a block matrix  $\begin{pmatrix} A \\ B \end{pmatrix}$  where  $A$  is  $\begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$  and  $B$  is  $\begin{pmatrix} 0 & 0 \end{pmatrix}$ . Row operations do not affect the  $e_i$ , but column operations do. Interchanging the two columns interchanges the  $e_i$ . A column operation  $c_i = c_i + kc_{i'}$  changes  $e_{i'}$  to  $e_{i'} - ke_i$ . Upon finishing, you should be left with  $e_1 = (3, 4)$  and  $e_2 = (6, 6)$ .  $\square$

4. [Jan 05 #3] Let  $R$  be a PID,  $p$  a prime element of  $R$  and  $M \neq \{0\}$  a finitely generated  $R$ -module such that there exists a natural number  $k$  with  $p^k M = \{0\}$ . We choose  $k$  minimal with this property, i.e.  $p^{k-1} M \neq \{0\}$ . (a) Describe the structure of  $M$ . Show that  $p^k$  is an elementary divisor of  $M$  and that each elementary divisor of  $M$  divides  $p^k$ . (b) Let  $m$  be any element of  $M$  with the property that  $p^{k-1} m \neq 0$ . Show that the cyclic module  $N := Rm$  has a complement  $C$  in  $M$ , i.e.  $M = N \oplus C$ .

*Proof.* (a) We are told that  $M$  is a torsion  $R$  module. By the structure theorem for finitely generated modules over PIDs, there are prime elements  $p_1, \dots, p_n \in R$ , and integers  $e_1, \dots, e_n \in \mathbb{N}$  such that  $M \cong \bigoplus_{i=1}^n R/(p_i^{e_i})$ . Now  $p^k M = 0$  iff  $p^k (R/(p_i^{e_i})) = 0$  for  $1 \leq i \leq n$ , which is in turn true iff  $p_i^{e_i} | p^k$  for  $1 \leq i \leq n$ . So each elementary divisor divides  $p^k$ . Now  $0 \neq p^{k-1} M \cong p^{k-1} (\bigoplus_{i=1}^n R/(p_i^{e_i})) \cong \bigoplus_{i=1}^n p^{k-1} (R/(p_i^{e_i}))$ . Since  $p^{k-1} (R/(p_i^{e_i})) \neq 0$  for some  $1 \leq i \leq n$ ,  $p_i^{e_i} = p^k$ . So  $p^k$  is an elementary divisor of  $M$ .

(b) Let  $m \in M$  with  $p^{k-1} m \neq 0$ . Say the isomorphism  $M \cong \bigoplus_{i=1}^n R/(p^{e_i})$  is given by  $\psi : \bigoplus_{i=1}^n R/(p^{e_i}) \rightarrow M$ . Let  $M_i = \psi(R/(p^{e_i}))$ , so  $M = \bigoplus_{i=1}^n M_i$ . Write  $m = \sum_{i=1}^n m_i$  with  $m_i \in M_i$ . Now  $0 \neq p^{k-1} m$  so  $p^{k-1} m_i \neq 0$  for some  $1 \leq i \leq n$ , say  $p^{k-1} m_n \neq 0$ . Note then  $\text{Ann}_R(m_n) = (p^k)$  because  $R$  is a PID,  $p^k \in \text{Ann}_R(m_n)$  and  $p^{k-1} \notin \text{Ann}_R(m_n)$ . Since  $M_n \cong R/(p^{e_n})$  is cyclic, there is an  $m' \in M$  such that  $M_n = Rm'$ . Claim:  $M_n = Rm_n$ . Then there is an  $r \in R$  such that  $m_n = rm'$ . Now  $(p, r) = 1$  or else  $p^{k-1} m_n = 0$ . Then  $(p^k, r) = 1$ , so there are  $x, y \in R$  such that  $1 = rx + p^k y$ . Then  $m' = (rx + p^k y)m' = x(rm') + y(p^k m') =$

$xm_n \in Rm_n$ , so  $M_n = Rm_n$ . To prove the claim, we have  $M = (\bigoplus_{i=1}^{n-1} M_i) \oplus Rm$ . Let  $N = \bigoplus_{i=1}^{n-1} M_i$ . If  $rm \in N$  then  $rm_n = 0$  so  $r \in \text{Ann}_R(m_n) = (p^k) = \text{Ann}_R(M)$ . So  $rm = 0$  implies that  $Rm \cap N = \{0\}$ . Let  $m' \in M$ , and write  $m' = \sum_{i=1}^n m'_i$ . Then  $m'_n \in Rm_n$ , and  $m'_n = rm_n$  for some  $r \in R$ . Then  $m' - rm = \sum_{i=1}^{n-1} (m'_i - rm_i) \in N$ , so  $m' \in N + Rm$ . Therefore,  $M = Rm \oplus C$  where  $C = \bigoplus_{i=1}^{n-1} M_i$ .  $\square$

5. [Aug 98 #4] Let  $a, b, c$  be distinct elements of an integral domain  $D$ . Show that there are *unique* elements  $x, y, z$  in  $D$  such that

$$\begin{aligned} x + y + z &= 0 \\ ax + by + cz &= 0 \\ a^2x + b^2y + c^2z &= 0 \end{aligned}$$

*Proof.* Use elementary row and column operations to get  $A$  to be

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & b-a & c-a \\ 0 & 0 & (c-a)(c-b) \end{pmatrix}$$

This matrix has determinant  $1(b-a)(c-a)(c-b) \neq 0$ . If we let  $\vec{x} = (x, y, z)^T$ , then  $A\vec{x} = 0$  implies that  $(c-a)(c-b)z = 0$  and so  $z = 0$ . This then implies  $(b-a)y = 0$ , so  $y = 0$ , and finally  $x = 0$ . So the unique solution is  $\vec{x} = 0$ .  $\square$

6. [Sept 86 #5] If  $M$  is an artinian module over a general  $R$ , show that any injective endomorphism is surjective.

*Proof.* Let  $M$  be an artinian  $R$ -module,  $\varphi : M \hookrightarrow M$  an injective  $R$ -module homomorphism. Suppose that  $\varphi$  is not surjective, so  $\varphi(M) \subsetneq M$ . Consider the decreasing sequence of ideals  $M = I_0 \supsetneq I_1 \supseteq I_2 \supseteq \cdots$  where  $I_i = \varphi^i(I_{i-1})$  for  $i \geq 1$ . Then there is an  $m \in \mathbb{N}$  such that  $I_j = I_m$  for  $j \geq m$  but  $I_{m-1} \neq I_m$ . Let  $p \in I_{m-1} \setminus I_m$ . Then  $\varphi(p) \in I_m = I_{m+1} = \varphi(I_m)$ , so there is a  $p' \in I_m$  such that  $\varphi(p) = \varphi(p')$ . But this contradicts that  $\varphi$  is injective.  $\square$

7. [Sept 84 #5] If  $A, B, C$  are submodules of a general  $R$ -module  $M$ , with  $A \supseteq C$ , show that  $A \cap (B + C) = (A \cap B) + C$ .

*Proof.* Let  $m \in A \cap (B + C)$ . Then there is a  $b \in B$  and  $c \in C$  such that  $m = b + c$ . But  $m \in A$  and  $C \subseteq A$  implies that  $b = m - c \in A$ . So  $b \in A \cap B$  and  $m \in (A \cap B) + C$ . Conversely, let  $m \in (A \cap B) + C$ . Then there is a  $d \in A \cap B$  and  $c \in C$  such that  $m = d + c$ . Now  $d \in A \cap B$  and  $c \in C \subseteq A$  implies that  $m = d + c \in A$ . Also,  $d \in B$  implies that  $m \in B + C$ . Then  $m \in A \cap (B + C)$ . Conclude that  $A \cap (B + C) = (A \cap B) + C$ .  $\square$

8. [Jan 87 #6; Aut 88#6] If  $I$  is an ideal of a commutative ring  $R$ , show (a)  $R/I$  is simple as an  $R$ -module iff  $I$  is a maximal ideal, (b) If  $I$  is prime then  $R/I$  is an indecomposable  $R$ -module, (c) If  $I$  is prime, what kind of *ring* is  $R/I$ ?

*Proof.* (a) If  $R/I$  is simple then the only submodules of  $R/I$  are 0 and  $R/I$ , so the only ideals of  $R/I$  are  $R/I$  and 0. Therefore, the only ideals of  $R$  containing  $I$  are  $I$  and  $R$ , so  $I$  is maximal. Conversely, if  $I$  is maximal, then  $R/I$  is a field, so the only ideals of  $R/I$  are 0 and  $R/I$ . Thus,  $R/I$  has no non-trivial submodules, so  $R/I$  is simple.

(b) Let  $I \trianglelefteq R$  be prime. Suppose  $R/I$  is decomposable, i.e. there are nonzero submodules  $M_1, M_2 < R/I$  such that  $R/I = M_1 \oplus M_2$ . Then  $M_1, M_2$  are merely ideals of  $R/I$ , so there are ideals  $J, K \trianglelefteq R$  containing  $I$  such that  $M_1 = J/I$  and  $M_2 = K/I$ . Let  $j \in J \setminus I$  and  $k \in K \setminus I$ . Then  $jk + I \in J/I \cap K/I = 0$  so  $jk \in I$ . But then  $j \in I$  or  $k \in I$ , a contradiction. Conclude that  $R/I$  is indecomposable.

(c) If  $I$  is prime then  $R/I$  is an integral domain. □

9. [Jan 98 #4] Let  $M$  be a module over a ring. A *section*  $A : B$  of  $M$  is a pair of submodules  $A, B$  of  $M$  with  $B \subseteq A$ ; a *trivial section* is where  $B = A$ . A submodule  $C$  of  $M$  *covers* a section  $A : B$  if  $(A \cap C) + B = A$  and *avoids*  $A : B$  if  $A \cap C \subseteq B$ . (a) Show that  $C$  covers  $A : B$  iff  $A \subseteq B + C$ , and avoids  $A : B$  iff  $A \cap (B + C) = B$ . (b) Show that every  $C$  simultaneously covers and avoids any trivial section; that any  $C$  with  $C \supseteq A$  covers  $A : B$ ; and that any  $C$  with  $C \subseteq B$  avoids  $A : B$ . (c) Give an example of a  $\mathbb{Z}$ -module  $M$  and a submodule  $C$  that covers one nontrivial section  $A : B$  and avoids another nontrivial section  $A' : B'$  for which the quotients  $A/B$  and  $A'/B'$  are isomorphic.

*Proof.* (a)  $A = (A \cap C) + B = A \cap (C + B)$  iff  $A \subseteq B + C$ . Similarly,  $A \cap C \subseteq B$  iff  $B = B + (A \cap C) = A \cap (B + C)$ .

(b) If  $A = B$  then for all  $C \leq M$ ,  $A \subseteq A + C = B + C$  and  $A \cap C \subseteq A = B$ . If  $A \subseteq C$  then  $A \subseteq B + C$ . If  $C \subseteq B$  then  $A \cap C \subseteq C \subseteq B$ .

(c)  $M = \mathbb{Z}, A = 3\mathbb{Z}, B = 9\mathbb{Z}, A' = 2\mathbb{Z}, B' = 6\mathbb{Z}, C = 3\mathbb{Z}$ . Then  $3\mathbb{Z} = A \subseteq 3\mathbb{Z} + 9\mathbb{Z} = B + C$ ,  $A' \cap C = 2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z} = B$ , and  $A/B \cong A'/B' \cong \mathbb{Z}_3$ . □

10. [Aug 96 #3] Let  $M$  be a finitely generated module over a ring  $R$ . Show that *any* generating set for  $M$  as an  $R$ -module must contain a *finite* generating set. Conclude that  $M$  has a minimal generating set (no proper subset generates  $M$ ), and that every minimal generating set of  $M$  is finite.

*Proof.* Say  $M = \langle m_1, m_2, \dots, m_s \rangle_R$ . Let  $N$  be a possibly infinite generating set for  $M$ . Then for each  $1 \leq i \leq s$  there is an  $n_i \in \mathbb{N}$  and  $m_{i,1}, m_{i,2}, \dots, m_{i,n_i} \in N$  and  $r_{i,1}, r_{i,2}, \dots, r_{i,n_i} \in R$  such that  $m_i = \sum_{j=1}^{n_i} r_{i,j} m_{i,j}$ . Let  $N' = \{m_{i,j} | 1 \leq i \leq s, 1 \leq j \leq n_i\}$ . Then  $N'$  is a finite

generating set for  $M$ . Let  $\mathcal{N} = \{A \subseteq M \mid \langle A \rangle_R = M \text{ and } |A| < \infty\}$ , which we now know is nonempty. Let  $n$  be the minimum of  $|A|$  for all  $A \in \mathcal{N}$ . Then if  $A \in \mathcal{N}$  with  $|A| = n$ ,  $A$  generates  $M$  but no proper subset of  $A$  generates  $M$  (by the minimality of  $|A|$ ). Any minimal generating set of  $M$  is finite because any infinite generating set is not minimal.  $\square$

11. [Aut 94 #8] If the *annihilator* of a left  $R$ -module  $M$  is  $\text{Ann}_R(M) = \{a \in R \mid aM = 0\}$ , show that for submodules  $M_1, M_2$  of  $M$  we have  $\text{Ann}_R(M_1 + M_2) = \text{Ann}_R(M_1) \cap \text{Ann}_R(M_2)$ . Show furthermore that we have  $\text{Ann}_R(M_1) + \text{Ann}_R(M_2) \subseteq \text{Ann}_R(M_1 \cap M_2)$ , but show that this inclusion could be strict. Additional question: Is  $\text{Ann}_R(M_1) + \text{Ann}_R(M_2) = \text{Ann}_R(M_1 \cap M_2)$  true if  $R$  is a PID and  $M$  is a finitely generated torsion  $R$ -module (no free summand)?

*Proof.*  $a(M_1 + M_2) = 0$  iff  $aM_1 + aM_2 = 0$  iff  $aM_1 = 0$  and  $aM_2 = 0$ , so  $a \in \text{Ann}_R(M_1 + M_2)$  iff  $a \in \text{Ann}_R(M_1) \cap \text{Ann}_R(M_2)$ . If  $a \in \text{Ann}_R(M_1)$  and  $b \in \text{Ann}_R(M_2)$ , and  $m \in M_1 \cap M_2$  then  $(a + b)m = am + bm = 0$ , so  $\text{Ann}_R(M_1) + \text{Ann}_R(M_2) \subseteq \text{Ann}_R(M_1 \cap M_2)$ . Consider the  $\mathbb{Z}$ -module  $M = A \oplus B$  where  $A = B = \mathbb{Z}_2$ . Then  $\text{Ann}_{\mathbb{Z}}(A) = \text{Ann}_{\mathbb{Z}}(B) = 2\mathbb{Z}$ ,  $\text{Ann}_{\mathbb{Z}}(A \cap B) = \text{Ann}_{\mathbb{Z}}(\{0\}) = \mathbb{Z}$ , and  $2\mathbb{Z} \subsetneq \mathbb{Z}$ . This example has  $R = \mathbb{Z}$  a PID and  $M$  a finitely generated torsion  $R$ -module.  $\square$

## 3.2 Rational and Jordan canonical form

Right.

# Chapter 4

## Fields

### 4.1 General Field Theory

1. [Feb 84 #6] If  $[F(a) : F]$  is odd show  $F(a^2) = F(a)$ .

*Proof.* Clearly  $F(a^2) \subseteq F(a)$ . Suppose  $a \notin F(a^2)$ . Then  $\mu_{a|F(a^2)}(t) = t^2 - a^2$ . So  $[F(a) : F] = [F(a) : F(a^2)][F(a^2) : F] = 2 \cdot [F(a^2) : F]$ , which is clearly not odd.  $\square$

2. [May 89 #3] If  $a, b$  are algebraic over  $F$  of degrees  $m, n$ , show  $[F(a, b) : F] \leq mn$ , with equality if  $m, n$  are relatively prime. Give an example where the inequality is strict.

*Proof.* We have  $[F(a, b) : F] = [F(a, b) : F(a)][F(a) : F]$  and  $[F(a, b) : F(a)] \leq [F(b) : F]$  because  $\mu_{b|F(a)} | \mu_{b|F}$ , so  $[F(a, b) : F] \leq mn$ . Also,  $[F(a, b) : F] = [F(a, b) : F(b)][F(b) : F]$ , so  $m, n | [F(a, b) : F]$ . If  $(m, n) = 1$  then  $mn | [F(a, b) : F]$ , i.e.  $mn = [F(a, b) : F]$ . Example:  $[\mathbb{Q}(\sqrt{2}, -\sqrt{2}) : \mathbb{Q}] = 2$  and  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(-\sqrt{2}) : \mathbb{Q}] = 2$ .  $\square$

3. [Aug 89#5] If  $[E : F]$  is finite, show any ring endomorphism of  $E$  which fixes  $F$  is an automorphism of  $E$ .

*Proof.* Let  $f \in \text{End}(E)$ . Then  $\ker(f) \trianglelefteq E$  so  $\ker(f) = \{0\}$  or  $\ker(f) = E$ . Since  $f|_F = id$ ,  $\ker(f) = \{0\}$  and  $f$  is injective. Then  $f(E)$  is a subfield of  $E$  containing  $F$ , and  $[E : F] = [E : f(E)][f(E) : F]$ . If we let  $n = [E : F] < \infty$ , and consider  $E$  as an  $F$ -vector space, then there are  $v_1, \dots, v_n \in E$  that form an  $F$ -basis for  $E$ . Then  $f(v_1), \dots, f(v_n)$  span  $f(E)$ . Moreover, if there are  $r_1, \dots, r_n \in F$  such that  $0 = r_1 f(v_1) + \dots + r_n f(v_n) = f(r_1 v_1 + \dots + r_n v_n)$ , then  $r_1 v_1 + \dots + r_n v_n = 0$  implies  $r_1 = r_2 = \dots = r_n = 0$ , so the  $f(v_i)$  are linearly independent. Conclude that  $[f(E) : F] = n$ , and hence  $[E : f(E)] = 1$ , i.e.  $E = f(E)$ , so  $f \in \text{Aut}(E)$ .  $\square$

4. [Aug 99 #8] If  $F$  is finite, show that every element  $\alpha \in F$  is the sum  $\alpha = \beta_1^2 + \beta_2^2$  of two squares (for some  $\beta_1, \beta_2 \in F$ ).

*Proof.* Consider the map  $\varphi : F^\times \rightarrow F^\times$  given by  $\varphi(a) = a^2$ . Then  $\ker(\varphi) = \{x \in F^\times \mid x^2 - 1 = 0\}$ . If  $\text{char}(F) = 2$ ,  $\ker(\varphi) = \{1\}$ , and  $\varphi(F^\times) = F^\times$ . If  $\text{char}(F) \neq 2$  then  $|\ker(\varphi)| = 2$  and  $|\varphi(F^\times)| = |F^\times / \ker(\varphi)| = (|F| - 1)/2$ . Say  $|F^\times| = p^n$ . Since  $0^2 = 0$ ,  $F$  has  $((p^n - 1)/2) + 1$  squares. Let  $\beta \in F^\times$ ,  $B = \{\beta - x^2 \mid x \in F\}$ . Then  $|B| = ((p^n - 1)/2) + 1$ . Now  $|F| = p^n \geq [((p^n - 1)/2) + 1] + [((p^n - 1)/2) + 1] - |\{x^2 \mid x \in F\} \cap \{\beta - y^2 \mid y \in F\}| = p^n + 1 - |\{x^2 \mid x \in F\} \cap \{\beta - y^2 \mid y \in F\}|$ . Then  $|\{x^2 \mid x \in F\} \cap \{\beta - y^2 \mid y \in F\}| \geq 1$ . So for some  $x, y \in F$ ,  $\beta = x^2 + y^2$ . If  $\text{char } F = 2$ , any  $\beta \in F$  satisfies  $\beta = \alpha^2 + 0^2$  for some  $\alpha \in F$ .  $\square$

5. [Aug 99 #5] Let  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$  ( $a_n \neq 0$ ) be a complex polynomial of degree  $n > 1$ , and  $f'$  its derivative. Let  $\alpha_1, \dots, \alpha_n$  be the  $n$  roots of  $f$  and  $\alpha'_1, \dots, \alpha'_{n-1}$  the  $n - 1$  roots of the derivative (listing each root as many times as its multiplicity). Show that the *average* of the roots of  $f$  equals the *average* of the roots of  $f'$ . (Hint: Use the relations between the coefficients of a polynomial and the roots of that polynomial).

*Proof.* Notice that  $\frac{1}{a_n} f$  has the same roots as  $f$ , and  $\frac{1}{na_n} f'$  has the same roots as  $f'$ . Given a monic polynomial  $x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$  with roots  $\lambda_1, \dots, \lambda_n$ , we know that  $c_{n-1} = -(\lambda_1 + \cdots + \lambda_n)$  simply by expanding the product  $x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 = \prod_{i=1}^n (x - \lambda_i)$ . Then  $\frac{1}{n}(\alpha_1 + \cdots + \alpha_n) = \frac{1}{n} \cdot \frac{-a_{n-1}}{a_n}$ , and  $\frac{1}{n-1}(\alpha'_1 + \cdots + \alpha'_{n-1}) = \frac{-1}{n-1} \cdot \frac{(n-1)a_{n-1}}{na_n} = -\frac{a_{n-1}}{na_n}$ , i.e. the averages are the same.  $\square$

6. [Nov 77 #4] Define *finite* extension and *algebraic* extension; does either imply the other?

*Proof.* A field extension  $E|F$  is finite if  $E$  is finite dimensional as a vector space over  $F$ . The field extension  $E|F$  is algebraic if for every  $\alpha \in E$ , there is an  $f \in F[x]$  such that  $f(\alpha) = 0$ . The extension  $\overline{\mathbb{Q}}|\mathbb{Q}$ , where  $\overline{\mathbb{Q}}$  is the set of all  $c \in \mathbb{C}$  that are algebraic over  $\mathbb{Q}$ , is an infinite algebraic extension, so algebraic does not imply finite. Suppose  $E|F$  is finite and let  $\alpha \in E$ . Suppose  $[E : F] = n$ . Then  $1, \alpha, \dots, \alpha^n$  must be linearly dependent over  $F$ , so there are  $r_0, r_1, \dots, r_n \in F$  such that  $0 = r_0 + r_1 \alpha + \cdots + r_n \alpha^n$ . Then  $0 = f(\alpha)$ , where  $f(x) = r_0 + r_1 x + \cdots + r_n x^n \in F[x]$ , so finite implies algebraic.  $\square$

7. [Ap 77 #4b] If  $p(x) \in F[x]$  is irreducible, SHOW there is a finite extension  $E|F$  containing a root of  $p(x)$ .

*Proof.* Assume that  $p$  is monic. Since  $p$  is irreducible,  $(p) \trianglelefteq F[x]$  is a maximal ideal, so  $F[x]/(p)$  is a field. Let  $E = F[x]/(p)$ . Then  $E$  is a finite dimensional  $F$ -vector space with basis  $\bar{1} = 1 + (p), \bar{x} = x + (p), \dots, \bar{x}^{n-1} = x^{n-1} + (p)$ , where  $n = \deg(p)$ . We also have the canonical embedding  $\iota : F \rightarrow E$  given by  $\iota(\beta) = \beta + (p)$ . So we may consider  $E$  as a finite algebraic extension of  $F$ . Moreover, if  $\alpha = x + (p)$ , then  $\alpha$  is a root of  $p$  in  $E$ .  $\square$

8. [Sep 83 #3] (a) Show any finite subgroup of  $F^*$  (the multiplicative group of invertible elements of  $F$ ) must be cyclic. (b) Give an example of a finite nonabelian group contained in  $R^*$  for a ring  $R$ .

*Proof.* Claim: If  $G$  is a finite abelian group such that  $|\{g \in G | g^d = 1\}| \leq d$  for every  $d$  dividing  $|G|$ , then  $G$  is cyclic. Reasoning: Let  $G$  be a finite abelian group,  $|G| = p_1^{n_1} \cdots p_r^{n_r}$  for distinct primes  $p_1, \dots, p_r$ . Then there are subgroups  $H_1, \dots, H_r \leq G$  with  $|H_i| = p_i^{n_i}$  and  $G \cong H_1 \times \cdots \times H_r$ . Suppose  $G$  is not cyclic. Then  $H_i$  is not cyclic for some  $1 \leq i \leq r$ . Say  $H_1$  is not cyclic. Then  $\text{ord}(h) | p_1^{n_1-1}$  for every  $h \in H_1$ . In particular,  $|\{g \in G | g^{p_1^{n_1-1}} = 1\}| \geq |H_1| = p_1^{n_1} > p_1^{n_1-1}$ .

(a) Let  $G$  be a finite subgroup of  $F^*$ . Since  $F$  is an integral domain, the polynomial  $x^d - 1$  has at most  $d$  roots in  $F$  (and hence at most  $d$  roots in  $G \subseteq F$ ) for each  $d$  dividing  $|G|$ . Then by the above claim,  $G$  is cyclic.

(b) Let  $R$  denote the ring of quaternions,  $R = \{a + bi + cj + dk | a, b, c, d \in \mathbb{R}\}$ . Then  $\{\pm 1, \pm i, \pm j, \pm k\}$ , the group  $Q_8$ , is a finite non-abelian group contained in  $R^*$ .  $\square$

9. [Aug 99 #9] If  $p$  is a prime number congruent to 1 mod 8, show that 2 is a “quadratic residue” mod  $p$ , i.e. there is an integer  $a$  such that  $a^2 \equiv 2 \pmod{p}$ . (Hint: show there is an  $\epsilon \in \mathbb{Z}_p$  with  $\epsilon^4 = -1$ , and consider  $\alpha = \epsilon + \epsilon^{-1}$ .)

*Proof.* For any  $\epsilon \in \mathbb{Z}_p$ ,  $(\epsilon + \epsilon^{-1})^2 = \epsilon^2 + 2 + \epsilon^{-2}$ . If for some  $\epsilon \in \mathbb{Z}_p$ ,  $\epsilon^4 = -1$ , then  $\epsilon^2 = \epsilon^{-2}\epsilon^4 = -\epsilon^{-2}$ , and for such an  $\epsilon$ ,  $(\epsilon + \epsilon^{-1})^2 \equiv 2 \pmod{p}$ . Suffices to show that there is an  $\epsilon \in \mathbb{Z}_p$  such that  $\epsilon^4 = -1$ . Now,  $x^{p-1} - 1$  splits over  $\mathbb{Z}_p$ . Since  $p \equiv 1 \pmod{8}$ ,  $\mathbb{Z}_p$  contains 8 distinct 8th roots of unity. Let  $\epsilon \in \mathbb{Z}_p$  be a primitive 8th root of unity. Then  $\epsilon^4 = -1$ .  $\square$

10. [Ap 77 #2] If  $F$  is finite SHOW (a)  $|F| = q$  is a power of a prime  $p$ , (b)  $F$  splits  $x^q - x$  over  $\mathbb{Z}_p$ , (c)  $F^*$  is cyclic of order  $q - 1$ .

*Proof.* (a) Let  $p \in \mathbb{N}$  be the smallest positive integer such that  $\overbrace{1 + \cdots + 1}^p = 0$ . Then  $p < \infty$  and  $p$  is a prime, because  $F$  is an integral domain. Then  $F$  contains a subfield isomorphic to  $\mathbb{Z}_p$ . Let  $n = [F : \mathbb{Z}_p]$ . Then  $|F| = p^n$ .

(b) Since  $F^*$  is cyclic,  $g^{q-1} - 1 = 0$  for every  $g \in F^*$ . Then  $g^q - g = 0$  for every  $g \in F$ . Also,  $\frac{d}{dx}(x^q - x) = qx^{q-1} - 1 = -1$ , so  $\text{gcd}(x^q - x, \frac{d}{dx}(x^q - x)) = 1$  and the roots of  $x^q - x$  are distinct. Conclude  $x^q - x$  splits over  $F$ .

(c) Given a field  $K$ , any finite subgroup of  $K \setminus \{0\}$  is cyclic. Then  $F^*$  is cyclic of order  $|F| - 1 = q - 1$ .  $\square$

11. [May 78 #10] Give a polynomial whose splitting field is a field of 9 elements; repeat for 18 elements.

*Proof.* Consider  $x^9 - x \in \mathbb{Z}_3[x]$ . Since  $\gcd(x^9 - x, \frac{d}{dx}(x^9 - x)) = \gcd(x^9 - x, -1) = 1$ ,  $x^9 - x$  is separable over  $\mathbb{Z}_3[x]$ . Let  $K = \{a_1, \dots, a_9\}$  be the roots of  $x^9 - x$ . Then  $1 \in K$  so  $\mathbb{Z}_3 \subseteq K$ . If  $a, b \in K$ ,  $(a + b)^9 - (a + b) = (a^9 + b^9) - (a + b) = (a + b) - (a + b) = 0$ ;  $(ab)^9 - ab = a^9b^9 - ab = ab - ab = 0$ ;  $(a^{-1})^9 - (a^{-1}) = (a^9)^{-1} - (a^{-1}) = a^{-1} - a^{-1} = 0$ . Conclude  $K$  is a field. Then  $x^9 - x$  splits over  $K$ , and  $|K| = 9$ . There are no fields of order 18 because 18 is not a prime power.  $\square$

12. [Sep 86 #1] If  $F = \mathbb{F}_7$ , show  $p(x) = x^2 + 1$  and  $q(x) = x^3 + x + 1$  are irreducible in  $F[x]$ , and show  $F[x]/(p(x))$  are fields (give their cardinalities).

*Proof.* If either of  $p(x)$  or  $q(x)$  are reducible over  $\mathbb{F}_7[x]$  then they must contain a root in  $\mathbb{F}_7$ . Check that this is not the case, so that  $p$  and  $q$  are irreducible. Then  $(p), (q) \trianglelefteq \mathbb{F}_7[x]$  are each maximal ideals, so  $\mathbb{F}_7[x]/(p)$  and  $\mathbb{F}_7[x]/(q)$  are each fields.  $|\mathbb{F}_7[x]/(p)| = 7^2$  and  $|\mathbb{F}_7[x]/(q)| = 7^3$ .  $\square$

13. [May 92 #6] Show that  $f(x, y) = x + x^3y + y^8 + x^7y^5 + x^2y^5$  is irreducible over the rational field.

*Proof.* We have that  $f \in F[x, y] = F[x][y]$  is irreducible by Eisenstein's criteria with the prime  $x \in F[x]$ . Then by Gauss' Lemma,  $f$  is irreducible in both  $\text{Frac}(F[x])[y]$  and  $\text{Frac}(F[y])[x]$ .  $\square$

14. [Jan 98 #6] The finite field  $\mathbb{F}_{32}$  of 32 elements can be constructed as the extension  $\mathbb{F}_2(\beta)$  where  $\beta$  is a root of the polynomial  $x^5 + x^2 + 1$  in  $\mathbb{F}_2[x]$ . Find the minimal polynomial of  $\beta^3$  over  $\mathbb{F}_2$ .

*Proof.* Note  $\beta^3 \in \mathbb{F}_2(\beta)$ ,  $[\mathbb{F}_2(\beta^3) : \mathbb{F}_2] \geq 2$  since  $[\mathbb{F}_2(\beta) : \mathbb{F}_2] = 5$ . This is because if  $[\mathbb{F}_2(\beta^3) : \mathbb{F}_2] = 1$ , then  $\beta^3 \in \mathbb{F}_2$  so  $\beta$  is a root of  $x^3 - \beta^3$  so  $[\mathbb{F}_2(\beta) : \mathbb{F}_2] \leq 3$ , which is a contradiction. But  $[\mathbb{F}_2(\beta^3) : \mathbb{F}_2]$  divides 5, so  $[\mathbb{F}_2(\beta^3) : \mathbb{F}_2] = 5$ . Consider  $x^5 + x^4 + x^3 + x^2 + 1$ .  $\square$

15. [Aug 94 #6] Show that  $F = \mathbb{F}_2[x]/(x^4 + x + 1)$  is a field of characteristic 2 containing a primitive 15th root of unity. Exhibit such a root.

*Proof.* Let  $f(x) = x^4 + x + 1$ . It suffices to show that  $f \in \mathbb{F}_2[x]$  is irreducible, for then  $(f) \trianglelefteq \mathbb{F}_2$  is a maximal ideal, and hence  $F$  is a field. Moreover, in this case  $F$  would have as an  $\mathbb{F}_2$ -basis the set  $\{\bar{1} = 1 + (f), \bar{x} = x + (f), \dots, \bar{x}^3 = x^3 + (f)\}$ . Then  $|F| = 2^4 = 16$ , so  $|F^\times| = 15$ . But  $F^\times$  is a cyclic group, say  $F^\times = \langle \beta \rangle$ . Then  $\beta^{15} - 1 = 0$ , and  $\beta$  is a primitive 15th root of unity. Now  $f(0) = f(1) = 1$ , so  $f$  is not divisible by any linear factors in  $\mathbb{F}_2[x]$ . The only irreducible quadratic in  $\mathbb{F}_2[x]$  is  $x^2 + x + 1$ , and  $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq f$ . Conclude that  $f$  is irreducible.  $\square$

16. [Sep 84 #7] Factor  $x^8 - 1$  into irreducibles in  $\mathbb{Z}_p[x]$  for *all* primes  $p$ .

*Proof.* We split into cases:

- If  $p = 2$ , then  $x^8 - 1 = (x - 1)^8$ .
- If  $p \equiv 1 \pmod{8}$ , then  $|\mathbb{Z}_p^*| = 8k$  for some  $k \in \mathbb{N}$ , and  $\mathbb{Z}_p$  must contain a primitive 8th root of unity  $\zeta_8$ , and  $x^8 - 1 = \prod_{i=1}^8 (x - \zeta_8^i)$ .
- If  $p \equiv 5 \pmod{8}$ , then  $p \equiv 1 \pmod{4}$  but  $p \not\equiv 1 \pmod{8}$ , so there is an  $i \in \mathbb{Z}_p^*$  such that  $i^2 = -1$ . Then  $x^8 - 1 = (x^2 + i)(x^2 - i)(x + i)(x - i)(x + 1)(x - 1)$ . [-1 is a square mod  $p$  iff  $p \equiv 1 \pmod{4}$ ]
- If  $p \equiv 7 \pmod{8}$ ,  $\zeta_8^4 = -1$ , primitive 8th root living in some extension of  $\mathbb{Z}_p$  and  $\zeta_8^4$  is a root of  $x^4 + 1$ . Now  $(x - \zeta_8)(x - \zeta_8^{-1}) = x^2 - x(\zeta_8 + \zeta_8^{-1}) + 1$ . Recall that  $\mathbb{Z}_p = \text{Fix}(\langle \sigma_p \rangle)$ , where  $\sigma_p$  is the Frobenius endomorphism, and  $\sigma_p(\zeta_8 + \zeta_8^{-1}) = \zeta_8^p + \zeta_8^{-p} = \zeta_8 + \zeta_8^{-1}$ . So  $\zeta_8 + \zeta_8^{-1} \in \mathbb{Z}_p$ , and  $(x - \zeta_8)(x - \zeta_8^{-1})$  splits over  $\mathbb{Z}_p$ . Now  $(x^4 + 1) = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$  where  $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$ .
- Finally, if  $p \equiv 3 \pmod{8}$ , then  $x^4 + 1 = (x^2 + \sqrt{-2}x - 1)(x^2 - \sqrt{-2}x - 1)$  where  $\sqrt{-2} = \zeta_8 + \zeta_8^3 \in \mathbb{Z}_p$  by the above Frobenius argument.

□

17. [Aug 89 #3] Show the set of all  $2 \times 2$  matrices  $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$  over  $\mathbb{F}_5$  form (under the usual matrix addition and multiplication) a field of size 25.

*Proof.* Let  $A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$  and  $C = \begin{pmatrix} c & d \\ 2d & c \end{pmatrix}$ . Then

$$A + C = \begin{pmatrix} a + c & b + d \\ 2(b + d) & a + c \end{pmatrix} \quad \text{and} \quad AC = \begin{pmatrix} ac + 2bd & ad + bc \\ 2(ad + bc) & ac + 2bd \end{pmatrix}$$

If  $A \neq 0$  then  $A^{-1} = \begin{pmatrix} e & f \\ 2f & e \end{pmatrix}$  where  $e = a/(a^2 - 2b^2)$  and  $f = -b/(a^2 - 2b^2)$ . Note that if  $a \neq 0$  and  $b \neq 0$ , then  $a^2 - 2b^2 \neq 0$ . Conclude that the set of all  $2 \times 2$  matrices  $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$  over  $\mathbb{F}_5$  forms a field of order 25. □

18. [1985 #3b] Show the set of all  $2 \times 2$  matrices  $\begin{pmatrix} a & b \\ \lambda b & a \end{pmatrix}$  over  $\mathbb{F}_7$  form (under the usual matrix addition and multiplication) a ring of size 49. For which  $\lambda \in \mathbb{F}_7$  is this a field?

*Proof.* Check that matrices of this form are closed under addition and multiplication. If  $\lambda \in \{3, 5, 6\}$ , then  $a^2 - \lambda b^2 \neq 0$  for every  $a, b \in \mathbb{F}_7$ , and so  $\begin{pmatrix} a & b \\ \lambda b & a \end{pmatrix}^{-1} = \begin{pmatrix} e & f \\ \lambda f & e \end{pmatrix}$  where  $e = a/(a^2 - \lambda b^2)$  and  $f = -b/(a^2 - \lambda b^2)$ . So the set is a ring (field if  $\lambda \in \{3, 5, 6\}$ ) of order 49. □

19. [Aut 04 #7] Consider the group  $G = SL_2(\mathbb{F}_4)$ . (a) Show *without* specifying any matrix that  $G$  contains an element of order 5. (b) Exhibit a concrete matrix  $A \in SL_2(\mathbb{F}_4)$  of order 5. Use  $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ , where  $\alpha$  is a root of  $x^2 + x + 1$ . Describe in detail how you obtained  $A$ ; you shouldn't just guess! (Hint: You might first factorize  $x^5 - 1$  in  $\mathbb{F}_4[x]$ ).

*Proof.* (a)  $|GL_2(\mathbb{F}_4)| = (4^2 - 1)(4^2 - 4) = 2^2 \cdot 3^2 \cdot 5$ . The map  $GL_2(\mathbb{F}_4) \xrightarrow{\det} \mathbb{F}_4^*$  has kernel  $SL_2(\mathbb{F}_4)$ , and so  $|SL_2(\mathbb{F}_4)| = 2^2 \cdot 3^2 \cdot 5 / (4 - 1) = 2^2 \cdot 3 \cdot 5$  ( $SL_2(\mathbb{F}_4) \cong A_4$ ). Since 5 divides  $|SL_2(\mathbb{F}_4)|$ , Cauchy's Theorem tells us there is an  $A \in G$  with  $\text{ord}(A) = 5$ .

(b) Let  $A \in G$  with  $\text{ord}(A) = 5$ . Then  $\mu_A | x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$ . Given  $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$  with  $\alpha^2 + \alpha + 1 = 0$ , we have  $\alpha^2 = \alpha + 1$ ,  $\alpha^3 = \alpha^2 + \alpha = 1$ , and  $\alpha^4 = \alpha$ . Since  $x^4 + x^3 + x^2 + x + 1 = (x^2 + \alpha x + 1)(x^2 + \alpha^2 x + 1)$ , this must be a factorization into irreducibles. (No element of  $\mathbb{F}_4$  can be a root of  $x^4 + x^3 + x^2 + x + 1$ , which is irreducible over  $\mathbb{F}_2$ , because then the degree of its minimal polynomial is too high). Pick  $A = \begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix}$ .  $\square$

20. [Sep 82 #4] If  $E|F$  is algebraic and each  $a \in E$  belongs to a normal sub-extension  $E_a$  ( $F \subseteq E_a \subseteq E$ ), show  $E|F$  is normal.

*Proof.* Let  $p(x) \in F[x]$  be irreducible. Suppose  $a \in E$  and  $p(a) = 0$ . Then there exists a normal subextension  $a \in E_a \subseteq E$ . Then  $p$  splits over  $E_a$  so  $p$  splits over  $E$ . Conclude  $E|F$  is normal.  $\square$

21. [Nov 77 #3] Give an example of an inseparable extension  $E|\mathbb{Q}$  of degree 7. If you don't succeed, give an arbitrary example of an algebraic but inseparable field extension.

*Proof.* Let  $E|\mathbb{Q}$  be a field extension of degree 7. Then  $E$  is algebraic over  $\mathbb{Q}$ . Let  $\beta \in E \setminus \mathbb{Q}$ . Since  $[\mathbb{Q}(\beta) : \mathbb{Q}]$  divides  $[E : \mathbb{Q}] = 7$  and  $\mathbb{Q}(\beta) \neq \mathbb{Q}$ , conclude  $[\mathbb{Q}(\beta) : \mathbb{Q}] = 7$  so  $E = \mathbb{Q}(\beta)$ . Let  $\mu(t)$  be the minimal polynomial of  $\beta$  over  $\mathbb{Q}$ . Then  $\mu$  is irreducible over  $\mathbb{Q}[t]$ . Then  $\gcd(\mu(t), \mu'(t)) = 1$  (because  $\mu'(t) \neq \mu(t)$  and  $\mu'(t) \neq 0$ ), so  $\mu$  is separable over  $\mathbb{Q}$ . Since  $\beta \in E \setminus \mathbb{Q}$  was arbitrary,  $E|\mathbb{Q}$  is separable. Conclude that every field extension of  $\mathbb{Q}$  of degree 7 is separable. In fact, every field extension of  $\mathbb{Q}$  is separable. Let  $K = \mathbb{F}_2(t)$  and  $L$  be the splitting field over  $K$  of  $x^2 - t$ . If  $\alpha^2 = t$ ,  $(x - \alpha)^2 = x^2 - 1$ .  $\square$

22. [Jan 95 #3] Let  $K$  and  $L$  be finite extensions of a field  $F$ , both contained in a field  $E$ . Let  $KL$  be the set of finite sums of products of members of  $K$  and  $L$ . Explain why  $KL$  is a subring of  $E$  that is finite dimensional over  $F$ . From that, show that  $KL$  is a field and, in fact, the smallest subfield of  $E$  containing  $K$  and  $L$ .

*Proof.* Let  $\{a_1, \dots, a_n\}$  be an  $F$ -basis for  $K$ , and let  $\{b_1, \dots, b_m\}$  be an  $F$ -basis for  $L$ . It is clear that  $0, 1 \in KL$  and  $KL$  is closed under addition and multiplication, hence is a subring of  $E$ . Moreover,  $KL$  is contained in the  $F$ -span of the set  $\{a_i b_j | 1 \leq i \leq n, 1 \leq j \leq m\}$ , so

$KL$  is evidently finite dimensional over  $F$ . So  $KL \subseteq F(a_1, \dots, a_n, b_1, \dots, b_m)$ . Have that  $F(a_1, \dots, a_n, b_1, \dots, b_m) = K(b_1, \dots, b_m)$ . But elements of  $K(b_1, \dots, b_m)$  are finite sums of the form  $\sum_i d_i b_m^i$ , with  $d_i \in K(b_1, \dots, b_{m-1})$ . So by induction, elements of  $K(b_1, \dots, b_m)$  can be written as elements of  $KL$ . Then  $KL = F(a_1, \dots, a_n, b_1, \dots, b_m)$  and  $KL$  is the smallest field containing  $K$  and  $L$ . [Let  $a \in KL$ . Since  $KL$  is finite dimensional over  $F$ ,  $a$  must be algebraic over  $F$ . Now  $a^{-1} \in F(a) = \{d_0 + d_1 a + \dots + d_k a^k \mid d_i \in F\} \subseteq KL$  for some  $k \in \mathbb{N}$ . Conclude that  $KL$  is a field containing  $K$  and  $L$ .]  $\square$

23. [Sep 93 #4] Prove that the additive group  $(F, +)$  of a field  $F$  can never be isomorphic to the multiplicative group  $(F^*, \cdot)$ . (Hint: consider orders of elements in the two groups)

*Proof.* If  $|F| < \infty$  then  $|F^\times| = |F| - 1 < |F|$ .

If  $|F| = \infty$  and  $1 = -1$ , suppose that  $f : F^\times \rightarrow (F, +)$  is an isomorphism. Then  $f(1) = 0$ . Also, for  $x \in F \setminus \{0\}$ ,  $f(x^2) = f(x) + f(x) = 0$  so  $x^2 = 1$  and  $x^2 - 1 = 0$ , telling us  $(x+1)(x-1) = 0$ , so that  $x = \pm 1$ , i.e.  $x = 1$ . Then  $F = \mathbb{F}_2$ , contradicting  $|F| = \infty$ .

If  $|F| = \infty$  and  $1 \neq -1$ , then for every  $x \in F \setminus \{0\}$ ,  $x \neq -x$ . Suppose  $f : (F, +) \rightarrow F^\times$  is an isomorphism. Let  $y \in F^\times \setminus \{1\}$ , and say  $y = f(x)$ . Then  $y \neq y^{-1}$  (or else  $x = -x$  by the injectivity of  $f$ ). But  $(-1)(-1) = 1$ , i.e.  $(-1)^{-1} = (-1)$ , contradiction.  $\square$

24. [Aug 97 #3] Let  $K(x)$  be the field of rational functions over the field  $K$ . Prove *Lüroth's Theorem*: for any constant function  $f \in K(x)$  the degree  $[K(x) : K(f)]$  is finite. Can you describe  $[K(x) : K(f)]$  in terms of  $f$ ?

*Proof.* Let  $f \in K(x) \setminus K$ . We can write  $f(x) = p(x)/q(x)$  for some  $p, q \in K[x]$  with  $(p, q) = (1)$ , and  $q(x) \neq 0$ . Consider  $h(t) \in K(f)[t]$ ,  $h(t) = q(t)f - p(t)$ . Then  $\deg(h) < \infty$ , and  $h(x) = q(x)f(x) - p(x) = p(x) - p(x) = 0$ , i.e.  $x$  is a root of  $h$ . Conclude  $[K(f)(x) : K(f)] = [K(x) : K(f)]$  is finite,  $[K(x) : K(f)]$  is no larger than the max of  $\deg(q)$  and  $\deg(p)$ .  $\square$

## 4.2 Galois Theory

1. [May 78 #11] Describe all intermediate fields of  $E|F$  if  $E|F$  is Galois with group  $\text{Gal}(E|F) = S_3$ .

*Proof.*  $\text{Fix}(S_3)$  corresponds to  $F$ .  $\text{Fix}(\langle(123)\rangle)$  is a normal extension of degree 2. There are 3 non-normal extensions of degree 3, corresponding to  $\text{Fix}(\langle(12)\rangle)$ ,  $\text{Fix}(\langle(13)\rangle)$ , and  $\text{Fix}(\langle(23)\rangle)$ . Finally,  $\text{Fix}(\{e\})$  corresponds to  $E$ .  $\square$

2. [Jan 92 #3] If  $\omega$  is a primitive cube root of 1, determine whether  $\mathbb{Q}(\omega\sqrt[3]{2})$  is a Galois extension of  $\mathbb{Q}$ . Give reasons.

*Proof.* Claim:  $\sqrt[3]{2} \notin \mathbb{Q}(\omega\sqrt[3]{2})$ . Reasoning: If  $\sqrt[3]{2} \in \mathbb{Q}(\omega\sqrt[3]{2})$ , then  $\omega \in \mathbb{Q}(\omega\sqrt[3]{2})$ . Then  $\mathbb{Q}(\omega, \sqrt[3]{2}) = \mathbb{Q}(\omega\sqrt[3]{2})$ . But  $[\mathbb{Q}(\omega, \sqrt[3]{2}), \mathbb{Q}] = 6 \neq 3 = [\mathbb{Q}(\omega\sqrt[3]{2}) : \mathbb{Q}]$ , so  $\sqrt[3]{2} \notin \mathbb{Q}(\omega\sqrt[3]{2})$ . Then  $x^3 - 2$  has a root in  $\mathbb{Q}(\omega\sqrt[3]{2})$  but doesn't split, so  $\mathbb{Q}(\omega\sqrt[3]{2})$  is not normal, and hence not Galois.  $\square$

3. [May 90 #3] If  $E|\mathbb{Q}$  is a finite Galois extension inside  $\mathbb{C}$  with  $\text{Gal}(E|\mathbb{Q})$  simple of order  $> 2$ , show the imaginary unit  $i$  CANNOT belong to  $E$ .

*Proof.* Note that  $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ . If  $i \in E$  then  $\mathbb{Q}(i)$  is a degree 2 subfield of  $E$ , so  $\text{Gal}(E|\mathbb{Q}(i))$  is an index 2 subgroup of  $\text{Gal}(E|\mathbb{Q})$ . But then  $\text{Gal}(E|\mathbb{Q}(i))$  is a proper non-trivial normal subgroup of  $\text{Gal}(E|\mathbb{Q})$ , which contradicts that  $\text{Gal}(E|\mathbb{Q})$  is simple.  $\square$

4. [May 89 #6] If  $E|F$  is Galois with  $\text{Gal}(E|F)$  simple, for any element  $a \in E$  which is not in  $F$  show that  $E$  is a splitting field for the minimum polynomial of  $a$  over  $F$ .

*Proof.* 7/10 #4  $\square$

5. [Fall 87 #8] If  $E|\mathbb{Q}$  is a splitting field of an irreducible polynomial  $f$  of degree 8, and  $a \in E$  is a root of  $f$  so that  $f$  splits over  $\mathbb{Q}(a)$  into 2 linear and 3 quadratic factors, find the possible orders of  $\text{Gal}(E|\mathbb{Q})$  and show that  $f$  is solvable by radicals.

*Proof.* Have  $[\mathbb{Q}(a) : \mathbb{Q}] = 8$ ,  $f$  splits as  $f = (x - a_1)(x - a_2)ghk$  over  $\mathbb{Q}(a)$  with  $g, h, k$  quadratics. Let  $b, c, d$  be roots of  $g, h, k$  respectively. Then  $f$  splits over  $E = \mathbb{Q}(a, b, c, d)$ ,  $|\text{Gal}(E|\mathbb{Q})| = [E : \mathbb{Q}] = 2^4, 2^5$ , or  $2^6$  (if  $c, d \in \mathbb{Q}(a, b)$ , if  $c \in \mathbb{Q}(a, b)$  and  $d \notin \mathbb{Q}(a, b)$ , or if  $c, d \notin \mathbb{Q}(a, b)$  and  $d \notin \mathbb{Q}(a, b, c)$ , respectively). [Note  $\text{char } \mathbb{Q} = 0$  implies  $f$  is separable.] So  $\text{Gal}(E|\mathbb{Q})$  is a  $p$ -group, hence nilpotent, so  $\text{Gal}(E|\mathbb{Q})$  is solvable, so  $f$  is solvable by radicals.  $\square$

6. [Aug 97 #1ac] Let  $p$  be a prime number and  $F$  a field containing  $p$  distinct  $p$ th roots of unity. Let  $E|F$  be a Galois extension for which  $[E : F] = p$ . (a) Prove that the Galois group  $\text{Gal}(E|F)$  is cyclic of order  $p$ . (b) Prove that there is an element  $b \in E|F$  with  $b^p \in F$ .

*Proof.* (a)  $|\text{Gal}(E|F)| = p$  implies  $\text{Gal}(E|F) \cong \mathbb{Z}_p$ .

(b) Let  $\zeta \in F$  be a primitive  $p$ -th root of unity,  $\sigma$  a generator of  $\text{Gal}(E|F)$ . For  $\alpha \in E$ , let  $(\zeta, \alpha) = \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{p-1}\sigma^{p-1}(\alpha)$ . Then  $\sigma((\zeta, \alpha)) = \sigma(\alpha) + \zeta\sigma^2(\alpha) + \cdots + \zeta^{p-1}\alpha = \zeta^{-1}(\zeta, \alpha)$ . Then  $\sigma((\zeta, \alpha)^p) = \zeta^{-p}(\zeta, \alpha)^p = (\zeta, \alpha)^p$ . In fact,  $\sigma^i((\zeta, \alpha)^p) = (\zeta, \alpha)^p$  for every  $1 \leq i \leq p - 1$ , so  $(\zeta, \alpha)^p \in \text{Fix}(\langle \sigma \rangle) = F$ . Since  $\sigma, \sigma^2, \dots, \sigma^{p-1}, id$  are linearly independent over  $F$ , there is an  $\alpha \in E$  such that  $(\zeta, \alpha) \neq 0$ . Then for such an  $\alpha$ ,  $\sigma^i(\zeta, \alpha) =$

$\zeta^{-i}(\zeta, \alpha) \neq (\zeta, \alpha)$  for  $1 \leq i \leq p-1$ . Conclude  $(\zeta, \alpha) \notin \text{Fix}(\langle \sigma \rangle) = F$ . Then  $b = (\zeta, \alpha) \in E|F$  satisfies  $b^p \in F$ . In fact,  $E = F(\sqrt[p]{b^p}) = F(b)$ .

Lemma: Above,  $id, \sigma, \dots, \sigma^{p-1}$  are linearly independent. Proof: Suppose not. Then some nontrivial  $F$ -linear combination  $a_1\sigma + a_2\sigma^2 + \dots + a_{p-1}\sigma^{p-1}$  is identically 0. Choose a minimal nontrivial combination  $a_1f_1 + \dots + a_mf_m$ . Since  $f_1 \neq f_m$  there is a  $g_0 \in E$  such that  $f_1(g_0) \neq f_m(g_0)$ . Then for every  $g \in E$ ,  $a_1f_1(g_0)f_1(g) + \dots + a_mf_m(g_0)f_m(g) = 0$ . Then

$$\begin{aligned} 0 &= [a_1f_1(g_0)f_1 + \dots + a_mf_m(g_0)f_m] - f_m(g_0)[a_1f_1 + \dots + a_mf_m] \\ &= (a_1f_1(g_0) - a_1f_m(g_0))f_1 + \dots + (f_{m-1}(g_0) - f_m(g_0))a_{m-1}f_{m-1} \end{aligned}$$

a dependence relation involving fewer nontrivial coefficients, contradicting our assumption. Conclude  $id, \sigma, \dots, \sigma^{p-1}$  are linearly independent.  $\square$

7. [1985 #4] Let  $E_n$  be the splitting field of  $x^n - 1$  over  $\mathbb{Q}$ . (a) What is  $[E_n : \mathbb{Q}]$ ? (b) What is  $|G_n|$  for  $G_n = \text{Gal}(E_n|\mathbb{Q})$ ? PROVE  $G_n$  is abelian. (c) SHOW  $G_{16}$  is not cyclic.

*Proof.* (a) Let  $\zeta$  denote a primitive  $n$ -th root of unity. Then  $E_n = \mathbb{Q}(\zeta)$ . Moreover, the minimal polynomial of  $\zeta$  over  $\mathbb{Q}$  has degree  $\varphi(n)$  (Euler's phi function), so  $[E_n : \mathbb{Q}] = \varphi(n)$ .

(b) Since  $E_n|\mathbb{Q}$  is a Galois extension,  $|G_n| = [E_n|\mathbb{Q}] = \varphi(n)$ . Note that  $\sigma \in G_n$  is completely determined by  $\sigma(\zeta)$ , and  $\sigma(\zeta)$  must be another primitive  $n$ -th root of unity. Let  $\psi : \mathbb{Z}_n^* \rightarrow G_n$  be given by  $\psi(a) = \sigma_a$ , where  $\sigma_a(\zeta) = \zeta^a$  and  $\sigma_a|_{\mathbb{Q}} = id_{\mathbb{Q}}$ . Then  $\sigma_a \in G_n$ , and  $\psi$  is well-defined (because  $\psi(a + nk) = \sigma_{a+nk}$  where  $\sigma_{a+nk}(\zeta) = \zeta^{a+nk} = \zeta^a = \sigma_a$ , i.e.  $\sigma_{a+nk} = \sigma_a$  for  $k \in \mathbb{Z}$ ). Also,  $\psi(ab) = \sigma_{ab}$  and  $\sigma_{ab}(\zeta) = \zeta^{ab} = (\zeta^b)^a = \sigma_a\sigma_b(\zeta)$ , i.e.  $\psi(ab) = \psi(a)\psi(b)$ . Then  $\mathbb{Z}_n^* \cong G_n$ , so  $G_n$  is abelian.

(c)  $G_{16} \cong \mathbb{Z}_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$  and  $\text{ord}(3) = \text{ord}(5) = \text{ord}(11) = \text{ord}(13) = 4 < 8$ ,  $\text{ord}(7) = \text{ord}(9) = \text{ord}(15) = 2 < 8$ .  $\square$

8. [May 80 #6] If  $F = \mathbb{Q}(\zeta)$  for a primitive  $n$ th root of unity  $\zeta$ , and  $b^n = a \in F$  where  $a \notin F^n$  is not an  $n$ th power in  $F$ , show  $G(F(b)|F)$  is abelian.

*Proof.* Since  $F$  contains all  $n$ -th roots of unity,  $x^n - a$  splits over  $F(b)$ . Hence  $F(b)|F$  is Galois. If  $\sigma \in G(F(b)|F)$ , then  $\sigma(b) = \zeta_\sigma b$  for some  $n$ -th root of unity  $\zeta_\sigma$ . Hence, define a map  $\varphi : G(F(b)|F) \rightarrow A$ , where  $A = \{\zeta \in \mathbb{C} | \zeta^n = 1\}$ , by  $\varphi(\sigma) = \zeta_\sigma$ . Now if  $\sigma, \tau \in G(F(b)|F)$ ,  $\sigma\tau(b) = \sigma(\zeta_\tau b) = \zeta_\tau\sigma(b) = \zeta_\tau\zeta_\sigma b = \zeta_\sigma\zeta_\tau b$ , so  $\varphi(\sigma\tau) = \zeta_\sigma\zeta_\tau = \varphi(\sigma)\varphi(\tau)$ . If  $\varphi(\sigma) = 1$ , then  $\sigma(b) = b$  so  $\sigma = id$ . Conclude  $\varphi$  is an injective homomorphism. Then  $G(F(b)|F)$  is abelian.  $\square$

9. [Aug 94 #7] Let  $\zeta_n$  be a primitive  $n$ th root of unit in  $\mathbb{C}$  for  $n > 2$ . (a) Show that the fixed field of  $\mathbb{Q}(\zeta_n)$  under complex conjugation is  $\mathbb{Q}(\zeta_n + \overline{\zeta_n}) = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$ . (Hint: write  $\overline{\zeta_n}$

as a power of  $\zeta_n$  and find a polynomial of low degree satisfied by  $\zeta_n$  over  $\mathbb{Q}(\zeta_n + \overline{\zeta_n})$ .) (b) For  $n = 7$ , find  $\text{Gal}(\mathbb{Q}(\zeta_7 + \overline{\zeta_7})|\mathbb{Q})$ , then find all subfields of  $\mathbb{Q}(\zeta_7)$  with their corresponding groups.

*Proof.* (a) Note that  $\zeta_n$  is a root of  $x^2 - x(\zeta_n + \zeta_n^{-1}) + 1 \in \mathbb{Q}(\zeta_n + \zeta_n^{-1})[x]$  and  $\overline{\zeta_n} = \zeta_n^{-1}$ , so  $|\text{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}(\zeta_n + \overline{\zeta_n}))| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \overline{\zeta_n})] = 2$ . Let  $\sigma$  be the complex conjugation map. Since  $\sigma(\zeta_n + \overline{\zeta_n}) = \zeta_n + \overline{\zeta_n}$ ,  $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}(\zeta_n + \overline{\zeta_n}))$ . But  $\text{ord}(\sigma) = 2$ , so  $\{id, \sigma\} = \text{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}(\zeta_n + \overline{\zeta_n}))$ . Then  $\text{Fix}(\langle \sigma \rangle) = \text{Fix}(\text{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}(\zeta_n + \overline{\zeta_n}))) = \mathbb{Q}(\zeta_n + \overline{\zeta_n})$ .

(b) Let  $E = \mathbb{Q}(\zeta_7)$ ,  $F = \mathbb{Q}(\zeta_7 + \overline{\zeta_7})$ . Have that  $\text{Gal}(E|\mathbb{Q}) \cong \mathbb{Z}_6$ ,  $\text{Gal}(E|F) = \langle \sigma_3 \rangle$ , where  $\sigma_3(\zeta_7) = \zeta_7^3$ . Then  $\mathbb{Z}_6 \leftrightarrow \mathbb{Q}$ ,  $\{1\} \leftrightarrow \mathbb{Q}(\zeta_7)$ ,  $\mathbb{Z}_3 \leftrightarrow \mathbb{Q}(\zeta_7 + \sigma_3^2(\zeta_7) + \sigma_3^4(\zeta_7)) = \mathbb{Q}(\zeta_7 + \zeta_7^2 + \zeta_7^4)$ ,  $\mathbb{Z}_2 \leftrightarrow \mathbb{Q}(\zeta_7 + \sigma_3^3(\zeta_7)) = \mathbb{Q}(\zeta_7 + \zeta_7^6) = \mathbb{Z}(\zeta_7 + \zeta_7^{-1})$ . Since  $\text{Gal}(E|\mathbb{Q})$  is abelian, all subfields of  $E$  containing  $\mathbb{Q}$  are normal. Then the map  $G(E|\mathbb{Q}) \rightarrow G(F|\mathbb{Q})$  given by  $\tau \mapsto \tau|_F$  induces the isomorphism  $G(E|\mathbb{Q})/G(E|F) \cong G(F|\mathbb{Q})$ , so  $G(F|\mathbb{Q}) \cong \mathbb{Z}_6/\mathbb{Z}_2 \cong \mathbb{Z}_3$ .  $\square$

10. [Jan 04 #5] Let  $\zeta$  be a primitive 9th root of unity. Let  $K = \mathbb{Q}(\zeta)$  and  $F = \mathbb{Q}(\zeta + \zeta^{-1})$ . (a) Show that  $[K : F] = 2$ . (b) Show that the extension  $F|\mathbb{Q}$  is normal.

*Proof.* (a) Note  $\zeta^{-1} = \overline{\zeta}$ , so  $\zeta + \zeta^{-1} \in \mathbb{R}$ . Then  $\zeta \notin F$ . But  $\zeta$  is a root of the polynomial  $x^2 - x(\zeta + \zeta^{-1}) + 1 \in F[x]$ . Conclude  $[K : F] = 2$ .

(b) Have  $[K : \mathbb{Q}] = \varphi(9) = 6$ , (Euler's phi), because  $\mu_{\zeta|\mathbb{Q}}(x)$  is a cyclotomic polynomial of degree  $\varphi(9)$ . Then  $[K : \mathbb{Q}] = [K : F][F : \mathbb{Q}]$ , so  $[F : \mathbb{Q}] = 3$ . Note that  $\text{Gal}(K|\mathbb{Q}) \cong \mathbb{Z}_9^* \cong \mathbb{Z}_6$ . Then every subgroup of  $\text{Gal}(K|\mathbb{Q})$  is normal, so every subfield of  $K$  containing  $\mathbb{Q}$  is normal.  $\square$

11. [Aug 04 #4] Let  $L|K$  be a finite Galois extension. Suppose there exists an element  $\alpha \in L$  and another root  $\alpha'$  of the minimal polynomial  $\mu_{\alpha|K}$  of  $\alpha$  over  $K$  such that the difference  $\alpha' - \alpha$  is an element of  $K \setminus \{0\}$ . (a) Prove that the characteristic  $p$  of  $K$  is different from 0 and that  $p$  divides  $[L : K]$ . (b) Give an example of an extension  $L|K$  and elements  $\alpha, \alpha'$  as described above.

*Proof.* (a) Say  $\alpha' = \alpha + b$ ,  $b \in K \setminus \{0\}$ . Now there is a  $\sigma \in \text{Gal}(L|K)$  such that  $\sigma(\alpha) = \alpha'$ . Then  $\sigma^2(\alpha) = \sigma(\alpha + b) = \sigma(\alpha) + b = \alpha + 2b$ , and  $\sigma^n(\alpha) = \alpha + nb$ . Since  $\text{ord}(\sigma) < \infty$ , must have  $\sigma^m(\alpha) = \alpha$  for some  $m \in \mathbb{N}$ . Then  $mb = 0$ , so  $\text{char}(K) > 0$ . Say  $\text{char}(K) = p$ . Then necessarily  $p | \text{ord}(\sigma)$ , so  $p$  divides  $|\text{Gal}(L|K)| = [L : K]$ .

(b) Let  $f = x^p - x + 1 \in \mathbb{F}_p[x]$ . If  $\alpha$  is a root of  $f$ , then  $f$  factors over  $\mathbb{F}_p(\alpha)$  as  $f = \prod_{i=1}^p (x - (\alpha + (i-1)))$ . Then  $\alpha - \alpha' \in \mathbb{F}_p \setminus \{0\}$  for  $\alpha \neq \alpha'$  roots of  $f$ .  $\square$

12. [Jan 87 #4] If  $F \subseteq K \subseteq E$  with  $K|F$  finite, show that if  $K|F$  is separable (resp. normal, Galois), then also  $K(a)|F(a)$  is separable (resp. normal, Galois) for any  $a \in E$ .

*Proof.* Let  $a \in E$ . Note that if  $\{v_1, \dots, v_n\}$  is an  $F$ -basis for  $K$ , then  $K(a)$  is contained in the  $F(a)$ -span of  $\{v_1, \dots, v_n\}$ , so  $[K(a) : F(a)] \leq [K : F] < \infty$ . Assume  $K(a) \neq F(a)$ , or else the results are true trivially.

(i) Suppose  $K|F$  is normal. Since  $[K : F] < \infty$ ,  $K$  is the splitting field of some  $f \in F[x] \setminus F$ . Say  $f$  has roots  $b_1, \dots, b_m \in K \setminus F$ . Then  $K = F(b_1, \dots, b_m)$ . Now  $K(a) = F(a, b_1, \dots, b_m)$ ,  $f$  as an element of  $F(a)[x]$  splits over  $K(a)$ , and not over any proper subfield containing  $F(a)$ . So  $K(a)$  is a splitting field for  $f \in F(a)[x]$ , and conclude that  $K(a)|F(a)$  is normal.

(ii) Suppose  $K|F$  is separable. Write  $K = F(b_1, \dots, b_m)$  for some  $b_1, \dots, b_m \in K \setminus F$ . Now  $\mu_{b_i|F}$  is separable implies that  $\mu_{b_i|F(a)}$  is separable because  $\mu_{b_i|F(a)}|\mu_{b_i|F}$ . Let  $\mathcal{B} = \{\mu_{b_i|F(a)} | 1 \leq i \leq m\}$  and let  $g = \prod_{f \in \mathcal{B}} f$ . Then  $g$  is separable. Let  $L$  be a splitting field for  $g$  over  $F$ . Then  $F(a) \subseteq K(a) \subseteq L$ . Moreover, the splitting field over  $F(a)$  of a separable polynomial is Galois. Then  $L|F(a)$  is separable, so  $K(a)|F(a)$  is separable.

(iii) If  $K|F$  is Galois, i.e. normal and separable, then  $K(a)|F(a)$  is normal and separable, i.e. Galois by (i) and (ii). □

13. [Aug 95 #6] Let  $E|\mathbb{Q}$  be splitting fields of  $x^3 - 9x + 12$ . Show that there is a single normal extension  $F|\mathbb{Q}$  with  $E \supseteq F \supseteq \mathbb{Q}$ . Find  $[F : \mathbb{Q}]$ .

*Proof.* The polynomial  $x^3 - 9x + 12$  is irreducible over  $\mathbb{Q}$  by Eisenstein's criterion with  $p = 3$ . It has one real root  $a$ , and two complex roots,  $b, \bar{b}$ . Then  $[E : \mathbb{Q}] = 6$ . Since  $3|[E : \mathbb{Q}] = |G(E|\mathbb{Q})|$ ,  $G(E|\mathbb{Q})$  contains a 3-cycle. Complex conjugation transposes  $b, \bar{b}$  and fixes  $a$ , so  $G(E|\mathbb{Q})$  contains a 2-cycle. But  $S_3$  is generated by any 3-cycle and 2-cycle, and  $G(E|\mathbb{Q})$  is isomorphic to a subgroup of  $S_3$ , so must be the whole group. A normal subextension  $F|\mathbb{Q}$  corresponds to a normal subgroup of  $S_3$ , of which there is precisely one:  $A_3$ . Then  $F = \text{Fix}(A_3)$ ,  $[F : \mathbb{Q}] = [S_3 : A_3] = 2$ . □

14. [Aug 98 #7] Suppose that  $K$  is a finite Galois extension of the rational field  $\mathbb{Q}$  which contains  $\sqrt{3}$  and has cyclic Galois group  $\text{Gal}(K|\mathbb{Q})$ . Show that  $L = \mathbb{Q}(\sqrt{3})$  is the only quadratic extension of  $\mathbb{Q}$  contained in  $K$ .

*Proof.* Let  $M$  be a quadratic extension of  $\mathbb{Q}$  contained in  $K$ . Then  $[\text{Gal}(K|\mathbb{Q}) : \text{Gal}(K|M)] = [M : \mathbb{Q}] = 2$ , so  $|\text{Gal}(K|M)| = \frac{1}{2}|\text{Gal}(K|\mathbb{Q})| = |\text{Gal}(K|L)|$ . Since  $\text{Gal}(K|\mathbb{Q})$  is cyclic, it has a unique subgroup of order  $|\text{Gal}(K|M)|$ . Then  $\text{Gal}(K|M) = \text{Gal}(K|L)$ , so  $L = \text{Fix}(\text{Gal}(K|L)) = \text{Fix}(\text{Gal}(K|M)) = M$ . □

15. [Jan 05 #6] Let  $f \in \mathbb{Q}[x]$  be an irreducible polynomial of degree 4,  $\alpha$  a root of  $f$ ,  $K = \mathbb{Q}(\alpha)$ , and  $L$  the splitting field of  $f$  over  $\mathbb{Q}$ . Assume that  $[L : \mathbb{Q}] \neq 4$ . (a) Show that  $G(L|\mathbb{Q})$  is isomorphic to  $S_4, A_4$ , or  $D_8$ . (b) Show that  $G(L|\mathbb{Q})$  is isomorphic to  $D_8$  if  $K$

contains a subfield  $F$  such that  $[F : \mathbb{Q}] = 2$ . (You might use the subgroup structure of  $S_4$  for free)

*Proof.* a) Since  $[L : \mathbb{Q}] \neq 4$ ,  $f$  factors over  $K$  as either (i) two linears and a quadratic, or (ii) a linear and a cubic. If (i), then  $[L : \mathbb{Q}] = 8 = |\text{Gal}(L|\mathbb{Q})|$  so  $\text{Gal}(L|\mathbb{Q})$  is isomorphic to a subgroup of  $S_4$  of order 8, so  $\text{Gal}(L|\mathbb{Q}) \cong D_8$ . If (ii), let  $\beta$  be a root of the cubic. Then  $f$  factors over  $K(\beta)$  as either (iii) 4 linears, or (iv) two linears and a quadratic. If (iii),  $[L : \mathbb{Q}] = 4 \cdot 3 = |\text{Gal}(L|\mathbb{Q})|$  so  $\text{Gal}(L|\mathbb{Q}) \cong A_4$ . If (iv),  $[L : \mathbb{Q}] = 4!$  so  $\text{Gal}(L|\mathbb{Q}) \cong S_4$ .

b) Assume  $K$  contains a subfield of  $F$  such that  $[F : \mathbb{Q}] = 2$ . Then  $F$  corresponds to an index 2 subgroup of  $\text{Gal}(L|\mathbb{Q})$ . Now  $A_4$  contains no index 2 subgroup, so  $\text{Gal}(L|\mathbb{Q}) \not\cong A_4$ . Note  $G(L|K) \leq G(L|\mathbb{Q})$  and  $G(L|K) \subseteq G(L|F)$ . If  $G(L|\mathbb{Q}) = 24$ , then  $G(L|\mathbb{Q})$  must contain a subgroup of order 6 contained in a normal subgroup of order 12. The only subgroup of  $S_4$  of order 12 is  $A_4$ , which contains no subgroup of order 6. Conclude  $G(L|\mathbb{Q}) \cong D_8$ .  $\square$

16. Let  $E$  be a separable extension of the field  $F$ , with  $[E : F] = n$ . Use Galois theory to find an upper bound  $B(n)$  for the number of intermediate fields  $K$ ,  $F \subseteq K \subseteq E$ , that depends only on  $n$ . You don't need to make the bound  $B(n)$  very tight!

*Proof.* By the primitive element theorem,  $E = F(\theta)$  for some  $\theta \in E$  with  $\deg(\mu_\theta) = n$ , where  $\mu_\theta \in F[x]$  is the minimal polynomial of  $\theta$  over  $F$ . Let  $E'$  be the splitting field of  $\mu_\theta$  over  $F$ . Then  $[E' : F] \leq (\deg(\mu_\theta))! = n!$ , so  $\text{Gal}(E'|F)$  is isomorphic to a subgroup of  $S_{n!}$ . There is a bijection between subgroups of  $S_{n!}$  and subfields  $L$  of  $E'$  containing  $F$ . In particular, there are no more intermediate fields  $K$  with  $F \subseteq K \subseteq E$  than there are subgroups of  $S_{n!}$ . So take  $B(n)$  to be the number of subgroups of  $S_{n!}$ .  $\square$

17. [Aug 96 #6] Let  $E|F$  be a finite Galois extension with Galois group  $G$ . The *Normal Basis Theorem* states that there is an element  $u$  in  $E$  whose image under the elements of  $G$  form an  $F$ -basis of  $E$ . Prove that for any subgroup  $H$  of  $G$ , the subfield corresponding to  $H$  in the Galois correspondence is  $F(u_H)$  for  $u_H = \sum_{h \in H} h(u)$ .

*Proof.* Let  $\sigma \in H$ . Then  $\{\sigma h | h \in H\} = H$ , so  $\sigma(u_H) = u_H$ , and  $\sigma$  fixes  $F(u_H)$ . Conversely, let  $\sigma \in G$  and suppose  $\sigma$  fixes  $F(u_H)$ . Then  $\sigma(u_H) = u_H$  implies  $\sigma(u) = h(u)$  for some  $h \in H$ , because  $\sigma$  permutes the basis elements  $\{g(u) | g \in G\}$ , and  $u = e(u)$  is a summand in  $u_H$ . Then  $h^{-1}\sigma(u) = u$  so  $h^{-1}\sigma = e$  because  $\{g(u) | g \in G\}$  is an  $F$ -linearly independent set. Then  $\sigma = h \in H$ . Conclude that  $F(u_H) = \text{Fix}(H)$  (since  $H = G(E|F(u_H))$ ), and so  $\text{Fix}(H) = \text{Fix}(G(E|F(u_H))) = F(u_H)$ .  $\square$

18. [Jan 95 #8] Give an example of a polynomial  $f(x) \in \mathbb{Q}[x]$  having all these properties: (1) degree 4; (2) no rational roots; (3) no repeated factors in  $\mathbb{Q}[x]$ ; (4) its Galois group over  $\mathbb{Q}$  is cyclic of order 2.

*Proof.* Suppose such an  $f \in \mathbb{Q}[x]$  that is monic exists, and let  $L$  be its splitting field. Let  $\alpha \in L$  be a root of  $f$ . If  $f$  is irreducible,  $4 = [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [L : \mathbb{Q}] = 2$ , which is clearly not possible, so  $f$  is reducible. Since  $f$  has no rational roots,  $f$  must factor as two quadratics,  $f = gh$  with  $\deg(g) = \deg(h) = 2$ . Let  $f(x) = (x - \sqrt{2})(x + \sqrt{2})(x - 2\sqrt{2})(x + 2\sqrt{2}) = (x^2 - 2)(x^2 - 8) = x^4 - 10x^2 + 16$ . Then  $L = \mathbb{Q}(\sqrt{2})$ ,  $\text{Gal}(L|\mathbb{Q}) \cong \mathbb{Z}_2$ .  $\square$

19. [Jan 98 #5b] The Galois group  $G$  of  $F$  of a polynomial  $f(x) \in F[x]$  of degree 4 is known to contain a subgroup isomorphic to the dihedral group  $D_8$ . (a) Show that  $f(x)$  is irreducible. (b) If some root  $r_i$  of  $f(x)$  lies in the subfield  $F(r_j, r_k)$  generated by two other roots, show  $F(r_j, r_k)$  is a splitting field for  $f(x)$  and that  $G = D_8$ .

*Proof.* (a)  $D_8 \leq \text{Gal}(f|F)$  implies that  $\text{Gal}(f|F)$  contains a 4 cycle, and so  $\text{Gal}(f|F)$  acts transitively on roots of  $f$ , so  $f$  is irreducible (roots can only be mapped to roots of some irreducible polynomial).

(b) Have  $r_i \in F(r_j, r_k)$ , so  $(x - r_i)(x - r_j)(x - r_k) | f$  in  $F(r_j, r_k)$ , and  $f$  splits over  $F(r_j, r_k)$ . But  $f$  does not split over  $F(r_j)$ , because  $[F(r_j) : F] = 4 < 8 \leq |G|$ . Conclude  $F(r_j, r_k)$  is a splitting field for  $f$ . Now  $f$  cannot factor over  $F(r_j)$  as 4 linears. If  $f$  factors over  $F(r_j)$  as a linear and a cubic ( $r_k$  a root of the cubic), then  $[F(r_j, r_k) : F] = 4 \cdot 3 = 12$ . But 8 does not divide 12. So  $f$  must factor over  $F(r_j)$  as two linears and a quadratic ( $r_k$  a root of the quadratic). Then  $[F(r_j, r_k) : F] = 8 = |G|$  so  $G \cong D_8$ .  $\square$

### 4.3 Finding Galois Groups

Given a polynomial  $f \in F[x]$ , respectively an element  $\beta$  which is algebraic over  $F$ , determine the Galois group  $G = G(f|F)$ , respectively  $G = G(F(\beta)|F)$  (also decide whether  $F(\beta)|F$  is Galois), and answer the questions in brackets.

1. [Jan 82 #II]  $F = \mathbb{Q}$ ,  $f = x^3 + 5x - 5$  (show  $f$  is irreducible, find its real roots; is  $G(f|\mathbb{Q})$  solvable?)

*Proof.*  $f$  is irreducible by Eisenstein's criterion with  $p = 5$ . Have  $f(0) = -5$ ,  $f(1) = 1$ ,  $f' = 3x^2 + 5$ , so we conclude that  $f$  has one real root at  $a$ . Then  $[\mathbb{Q}(a) : \mathbb{Q}] = 3$ , so 3 divides  $|G(f|\mathbb{Q})|$ , so  $G(f|\mathbb{Q})$  contains an element of order 3 (a 3-cycle), and  $|G(f|\mathbb{Q})| \leq 3!$ . Also,  $G(f|\mathbb{Q})$  contains the 2-cycle complex conjugation. Then  $G(f|\mathbb{Q}) \cong S_3$ , a solvable group. Conclude that  $f$  is solvable by radicals.  $\square$

2. [Ap 77 #6]  $F = \mathbb{Q}$ ,  $f = x^3 + 5$  (show  $f$  is irreducible but  $G$  is not of order 3; is  $G(f|\mathbb{Q})$  solvable?)

*Proof.*  $f$  has no rational roots, hence is irreducible over  $\mathbb{Q}$ . Note that  $f$  has the roots  $\omega, \sqrt[3]{5}, \omega_2\sqrt[3]{5}, \omega_3\sqrt[3]{5}$ , where  $\omega_1, \omega_2, \omega_3$  are roots of the polynomial  $x^3 + 1 = (x + 1)(x^2 - x + 1)$ , i.e.  $\omega_1 = -1, \omega_2 = \frac{1}{2} + \frac{\sqrt{3}}{2}i, \omega_3 = \frac{1}{2} - \frac{\sqrt{3}}{2}i$ . So  $f$  is solvable by radicals, and splits over  $\mathbb{Q}(\sqrt[3]{5}, i\sqrt{3})$ . Note that  $i\sqrt{3}$  satisfies  $x^2 + 3$ , which is irreducible over  $\mathbb{R}$  (and hence over  $\mathbb{Q}(\sqrt[3]{5})$ ). Then  $[\mathbb{Q}(\sqrt[3]{5}, i\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{5}, i\sqrt{3}) : \mathbb{Q}(\sqrt[3]{5})][\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 2 \cdot 3 = 6$ . Now  $G \cong S_3$  or  $G \cong \mathbb{Z}_6$ . But  $\mathbb{Q}(\sqrt[3]{5})$  is not normal, so  $G$  contains a non-normal subgroup of index 3, so  $G \cong S_3$ . We have the correspondence

$$\begin{aligned}\mathbb{Q}(\sqrt[3]{5}, i\sqrt{3}) &\leftrightarrow \{e\} \\ \mathbb{Q}(\sqrt[3]{5}), \mathbb{Q}(\omega_2\sqrt[3]{5}), \mathbb{Q}(\omega_3\sqrt[3]{5}) &\leftrightarrow \langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle \\ \mathbb{Q}(i\sqrt{3}) &\leftrightarrow \langle(123)\rangle \\ \mathbb{Q} &\leftrightarrow S_3\end{aligned}$$

□

3. [Aug 88 #5; Sep 80 #7]  $F = \mathbb{Q}, f = x^4 - x^2 - 6$ .

*Proof.*  $f = (x^2 - 3)(x^2 + 2) = (x - \sqrt{3})(x + \sqrt{3})(x - i\sqrt{2})(x + i\sqrt{2})$ , so  $f$  splits over  $E = \mathbb{Q}(\sqrt{3}, i\sqrt{2})$ . Since  $x^2 + 2$  has no real roots (and hence no roots in  $\mathbb{Q}(\sqrt{3})$ ), conclude  $[E : F] = [E : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 4$ . In fact,  $G(E|F) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ , with the three non-identity elements  $\sigma : \begin{smallmatrix} \sqrt{3} \rightarrow \sqrt{3} \\ i\sqrt{2} \rightarrow -i\sqrt{2} \end{smallmatrix}, \tau : \begin{smallmatrix} \sqrt{3} \rightarrow -\sqrt{3} \\ i\sqrt{2} \rightarrow -i\sqrt{2} \end{smallmatrix}$ , and  $\gamma = \sigma\tau$ . Thus we have the correspondence:

$$\begin{aligned}\mathbb{Q}(\sqrt{3}, i\sqrt{2}) &\leftrightarrow \{e\} \\ \mathbb{Q}(\sqrt{3}), \mathbb{Q}(i\sqrt{2}), \mathbb{Q}(i\sqrt{6}) &\leftrightarrow \langle\sigma\rangle, \langle\tau\rangle, \langle\gamma\rangle \\ \mathbb{Q} &\leftrightarrow \{e, \sigma, \tau, \gamma\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2\end{aligned}$$

□

4. [Jan 87 #3]  $F = \mathbb{Q}, f = x^4 - x^2 - 2$ .

*Proof.*  $f = (x^2 - 2)(x^2 + 1) = (x - \sqrt{2})(x + \sqrt{2})(x + i)(x - i)$  splits over  $E = \mathbb{Q}(i, \sqrt{2})$ , and  $[E : F] = 4$  ( $x^2 + 1$  has no roots in  $\mathbb{Q}(\sqrt{2})$ ). Have  $Gal(E|F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ . We have  $E \leftrightarrow \{e\}$ ,  $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(i) \leftrightarrow \mathbb{Z}_2$ , and  $\mathbb{Q} \leftrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ . □

5. [Sep 86 #4]  $F = \mathbb{Q}, f = x^4 + 1$ .

*Proof.*  $f = (x^2 + i)(x^2 - i) = (x - e^{\pi i/4})(x + e^{\pi i/4})(x - e^{-\pi i/4})(x + e^{-\pi i/4})$  and  $e^{\pi i/4} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ . Then  $E = \mathbb{Q}(\sqrt{2}, i)$ ,  $[E : F] = 4$ ,  $Gal(E|F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ . The correspondence is  $\mathbb{Q}(\sqrt{2}, i) \leftrightarrow \{e\}$ ,  $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(i) \leftrightarrow \mathbb{Z}_2$ , and  $\mathbb{Q} \leftrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ . □

7. [May 91 #5]  $F = \mathbb{Q}, f = x^4 - 2$  (find  $G$ , identify all subfields of degree 4 over  $\mathbb{Q}$  with their corresponding subgroups).

*Proof.*  $f = (x^2 - \sqrt{2})(x^2 + \sqrt{2}) = (x + \sqrt[4]{2})(x - \sqrt[4]{2})(x + i\sqrt[4]{2})(x - i\sqrt[4]{2})$  which splits over  $E = \mathbb{Q}(i, \sqrt[4]{2})$ . Then  $[E : F] = 8$ . Consider  $\sigma, \tau \in G(E|F)$ , where  $\sigma : \sqrt[4]{2} \mapsto i\sqrt[4]{2}$  and  $\tau : \sqrt[4]{2} \mapsto \sqrt[4]{2}$ . Then  $\text{ord}(\sigma) = 4$ ,  $\text{ord}(\tau) = 2$ , and  $\tau\sigma = \sigma^{-1}\tau$ . Since  $|\langle\sigma\rangle\langle\tau\rangle| = 8$  ( $\langle\sigma\rangle \trianglelefteq G$  because  $[G : \langle\sigma\rangle] = 2$ ). Conclude  $G \cong D_8$ . We have the following pairings:  $\mathbb{Q}(i, \sqrt[4]{2}) \leftrightarrow \{e\}$ ,  $\mathbb{Q} \leftrightarrow \langle\sigma, \tau\rangle$ ,  $\mathbb{Q}(i) \leftrightarrow \langle\sigma\rangle$ ,  $\mathbb{Q}(\sqrt{2}) \leftrightarrow \langle\tau, \sigma^2\rangle$ ,  $\mathbb{Q}(i\sqrt{2}) \leftrightarrow \langle\tau\sigma, \sigma^2\rangle$ ,  $\mathbb{Q}(\sqrt[4]{2}) \leftrightarrow \langle\tau\rangle$ ,  $\mathbb{Q}(i\sqrt[4]{2}) \leftrightarrow \langle\tau\sigma^2\rangle$ ,  $\mathbb{Q}(i, \sqrt{2}) \leftrightarrow \langle\sigma^2\rangle$ ,  $\mathbb{Q}((1+i)\sqrt[4]{2}) \leftrightarrow \langle\tau\sigma^2\rangle$ , and  $\mathbb{Q}((1-i)\sqrt[4]{2}) \leftrightarrow \langle\tau\sigma\rangle$ . One might argue that  $[\mathbb{Q}((1 \pm i)\sqrt[4]{2}) : \mathbb{Q}] = 4$  because  $\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(i, (1 \pm i)\sqrt[4]{2})$  and so  $[\mathbb{Q}(i, (1 \pm i)\sqrt[4]{2}) : \mathbb{Q}] \geq 4$ .  $\square$

9. [Aug 95 Comprehensive #3]  $F = \mathbb{Q}, f = x^4 - 4$  (describe  $G$  as automorphisms, find all subfields).

*Proof.*  $f = (x^2 + 2)(x^2 - 2) = (x + \sqrt{2})(x - \sqrt{2})(x + i\sqrt{2})(x - i\sqrt{2})$  splits over  $E = \mathbb{Q}(\sqrt{2}, i)$ . Then  $[E : F] = 4$  and  $G(E|F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ . Letting  $\sigma_1 = id$ ,  $\sigma_2 : \sqrt{2} \mapsto -\sqrt{2}$ ,  $\sigma_3 = \sqrt{2} \mapsto \sqrt{2}$ , and  $\sigma_4 = \sigma_2\sigma_3$ , we have the pairings:  $\mathbb{Q}(\sqrt{2}, i) \leftrightarrow \{e\}$ ,  $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(i\sqrt{2}), \mathbb{Q}(i) \leftrightarrow \mathbb{Z}_2$ , and  $\mathbb{Q} \leftrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ .  $\square$

11. [Jan 97 #5]  $F = \mathbb{Q}, f = x^4 - 5$  (describe  $G$  as a group of permutations of the roots).

*Proof.*  $f = (x^2 - \sqrt{5})(x^2 + \sqrt{5}) = (x - \sqrt[4]{5})(x + \sqrt[4]{5})(x - i\sqrt[4]{5})(x + i\sqrt[4]{5})$  splits over  $E = \mathbb{Q}(\sqrt[4]{5}, i)$ . We have  $[E : F] = 8$  with  $G \cong D_8$ . Let  $\sigma : \sqrt[4]{5} \mapsto i\sqrt[4]{5}$  and  $\tau : \sqrt[4]{5} \mapsto \sqrt[4]{5}$ . Then  $\sigma^4 = \tau^2 = id$  and  $\tau\sigma = \sigma^3\tau$ . We have the pairings:  $\mathbb{Q}(i, \sqrt[4]{5}) \leftrightarrow \{e\}$ ,  $\mathbb{Q}(i) \leftrightarrow \langle\sigma\rangle$ ,  $\mathbb{Q}(\sqrt{5}) \leftrightarrow \langle\tau, \sigma^2\rangle$ ,  $\mathbb{Q}(i\sqrt{5}) \leftrightarrow \langle\tau\sigma, \sigma^2\rangle$ ,  $\mathbb{Q}(\sqrt[4]{5}) \leftrightarrow \langle\tau\rangle$ ,  $\mathbb{Q}(i\sqrt[4]{5}) \leftrightarrow \langle\tau\sigma^2\rangle$ ,  $\mathbb{Q}(i, \sqrt{5}) \leftrightarrow \langle\sigma^2\rangle$ ,  $\mathbb{Q}((1+i)\sqrt[4]{5}) \leftrightarrow \langle\tau\sigma^3\rangle$ , and  $\mathbb{Q}((1-i)\sqrt[4]{5}) \leftrightarrow \langle\tau\sigma\rangle$ .  $\square$

12. [Sep 78 #4] (a) If  $f$  is irreducible of degree 5 over  $\mathbb{Q}$ , show  $G(f|\mathbb{Q})$  contains an element of order 5. (b) Show  $G(x^4 + 1|\mathbb{Q})$  has NO element of order 4.

*Proof.* (a) Let  $\alpha \in \mathbb{C}$  be a root of  $f$ . Then if  $L$  is a splitting field for  $f$  over  $\mathbb{Q}$ ,  $5 = [\mathbb{Q}(\alpha) : \mathbb{Q}] | [L : \mathbb{Q}] = |G(L|\mathbb{Q})|$ , so  $G(L|\mathbb{Q})$  contains an element of order 5.

(b)  $x^4 + 1 = 0$  implies  $x^4 = -1$ , which implies  $x = e^{\pi i/4 + 2\pi i k/4}$  for  $k = 0, 1, 2, 3$ . That is,  $x \in \{e^{\pi i/4}, e^{3\pi i/4}, e^{5\pi i/4}, e^{7\pi i/4}\} = \{\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\}$ . So  $x^4 + 1$  splits over  $L = \mathbb{Q}(\sqrt{2}, i)$ , and  $Gal(L|\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ . Then  $G(x^4 + 1|\mathbb{Q})$  contains no elements of order 4.  $\square$

14. [Mar 83 #2]  $F = \mathbb{Q}, \beta = (1 + \sqrt{2})/(1 + \sqrt{3})$ .

*Proof.*  $[\mathbb{Q}(\beta) : \mathbb{Q}(\sqrt{3})] = 2$  because  $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$ . Then we have  $[\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 4$ . Now  $\beta \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ , and  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ . Conclude  $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ , hence  $\mathbb{Q}(\beta)|\mathbb{Q}$  is Galois, and  $\text{Gal}(\mathbb{Q}(\beta)|\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ .  $\square$

15. [Sep 93 #6]  $F = \mathbb{Q}$ ,  $f = x^5 - 6x + 3$ . Prove  $f$  is (a) irreducible, (b) has exactly 3 real roots, (c)  $G(E|L)$  contains a transposition of roots of  $f$  for any real subfield  $L$  of the splitting field  $E$  of  $f$  over  $\mathbb{Q}$ , (d)  $G(E|\mathbb{Q}) = S_5$ .

*Proof.* (a)  $f$  is Eisenstein with  $p = 3$ , hence irreducible in  $\mathbb{Z}[x]$  and  $\mathbb{Q}[x]$ .

(b)  $f(-2) = -17$ ,  $f(-1) = 8$ ,  $f(1) = -2$ ,  $f(2) = 23$ , so  $f$  has real roots in  $(-2, -1)$ ,  $(-1, 1)$ , and  $(1, 2)$ . Note  $f'(x) = 5x^4 - 6 > 0$  for  $|x| \geq 2$ , so  $f$  has no real roots in  $(-\infty, -2) \cup (2, \infty)$ . Also,  $f''(x) = 20x^3$  is  $\leq 0$  for  $x \leq 0$ , is  $\geq 0$  for  $x \geq 0$ . Conclude  $f$  has exactly 3 real roots.

(c) Complex conjugation transposes the two complex roots of  $f$ , but leaves any real subfield  $L$  of  $E$  fixed.

(d) 5 divides  $|\text{Gal}(f|\mathbb{Q})|$  so  $\text{Gal}(f|\mathbb{Q})$  contains a 5-cycle. Complex conjugation corresponds to a 2-cycle in  $\text{Gal}(f|\mathbb{Q})$ . A 2-cycle and a 5-cycle generate  $S_5$ .  $\square$

17. [Jan 81 #2]  $F = \mathbb{Q}$ ,  $\beta$  a primitive 7th root of unity (find the minimum polynomial of  $\beta$ , find  $[\mathbb{Q}(\beta) : \mathbb{Q}]$ , find all subfields).

*Proof.*  $\beta$  satisfies  $x^7 - 1 = (x - 1)(x^6 + x^5 + \cdots + x + 1)$ . Let  $\mu(x) = x^6 + \cdots + x + 1$ . Then  $\mu(\beta) = 0$ , and  $\mu$  is irreducible over  $\mathbb{Q}$  (consider  $\mu(x+1)$ , which is Eisenstein with  $p = 7$ ). Then  $\mu$  splits over  $E = \mathbb{Q}(\beta)$ ,  $[E : \mathbb{Q}] = 6$ . Let  $G = \text{Gal}(E|\mathbb{Q})$ . Given  $\sigma \in G$ ,  $\sigma(\zeta) = \zeta^n$  for some  $1 \leq n \leq 6$ . Let  $\psi : \mathbb{Z}_6 \rightarrow G$  be defined by  $\psi(n) = \sigma_n$  where  $\sigma_n(\zeta) = \zeta^n$  and  $\sigma_n|_{\mathbb{Q}} = \text{id}_{\mathbb{Q}}$ . Then  $\psi$  is a well-defined map (note that  $\zeta^{n+7k} = \zeta^n$ ). Also,  $\sigma_{nm}(\zeta) = \zeta^{nm} = (\zeta^m)^n = \sigma_n \sigma_m(\zeta)$ , so  $\psi$  is a homomorphism and  $G \cong \mathbb{Z}_6$ . Then  $E$  has 4 subfields (because  $\mathbb{Z}_6$  has 4 subgroups). Now  $G = \langle \sigma_3 \rangle$ , and  $G$  has subgroups  $\{e\}, \langle \sigma_3^2 \rangle, \langle \sigma_3 \rangle$ . Then the intermediate fields are  $\mathbb{Q}, \mathbb{Q}(\zeta), \mathbb{Q}(\zeta + \zeta^{3^2} + \zeta^{3^4}) = \mathbb{Q}(\zeta + \zeta^2 + \zeta^4), \mathbb{Q}(\zeta + \zeta^{3^3}) = \mathbb{Q}(\zeta + \zeta^6) = \mathbb{Q}(\zeta + \zeta^{-1}), [\mathbb{Q}(\alpha_H), \alpha_H = \sum_{\sigma \in H} \sigma(\zeta)]$ .  $\square$

18. [Now 77 #8] Find  $\text{Gal}(E|\mathbb{Q})$  if  $E = \mathbb{Q}(i, \beta)$  for  $\beta$  a primitive  $n$ th root of unity for odd  $n > 1$ .

*Proof.* Note that  $i\beta$  is a primitive  $4n$ -th root of unity. Then  $E = \mathbb{Q}(i\beta)$ . Let  $\zeta = i\beta, G = \text{Gal}(E|\mathbb{Q})$ . Note that for each  $\sigma \in G$ ,  $\sigma$  is uniquely determined by  $\sigma(\zeta)$ , and  $\sigma(\zeta) = \zeta^m$  for some  $1 \leq m < 4n$  with  $(m, 4n) = 1$ . Moreover, for each  $1 \leq m < 4n$  with  $(m, 4n) = 1$ ,  $\sigma_m$  defined by  $\sigma_m(\zeta) = \zeta^m$  is an element of  $G$ . Also note that  $|G| = [E : \mathbb{Q}] = \varphi(4n)$  (Euler's phi function). Then  $\psi : \mathbb{Z}_{4n}^* \rightarrow G$ ,  $\psi(a) = \sigma_a$  is a well-defined bijection, and  $\sigma_a \sigma_b(\zeta) = (\zeta^b)^a = \zeta^{ab} = \sigma_{ab}(\zeta)$ , so  $\psi$  is a homomorphism, and  $\text{Gal}(E|\mathbb{Q}) \cong \mathbb{Z}_{4n}^*$ .  $\square$

19. [Jan 79 #6; Sep 79 #6] Find  $Gal(E|\mathbb{Q})$  for  $E = \mathbb{Q}(\sqrt{2}, i)$  or  $E = \mathbb{Q}(i + \sqrt{2})$ .

*Proof.* First, note that  $i, \sqrt{2}$  are separable over  $\mathbb{Q}$  and  $1 \notin \{0, \frac{-\sqrt{2}-\sqrt{2}}{i-(-i)} = \frac{-2\sqrt{2}}{2i} = i\sqrt{2}\}$ , so  $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i + \sqrt{2})$ . Note that  $i \notin \mathbb{Q}(\sqrt{2})$ , so  $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$ . Also,  $E$  is the splitting field over  $\mathbb{Q}$  of  $(x^2 + 1)(x^2 - 2)$ , and  $Gal(fg|\mathbb{Q})$  is isomorphic to a subgroup of  $Gal(f|\mathbb{Q}) \times Gal(g|\mathbb{Q})$ . Conclude  $G(E|\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ . We have the pairings:  $E \leftrightarrow \{e\}, \mathbb{Q}(\sqrt{2}) \leftrightarrow \mathbb{Z}_2, \mathbb{Q}(i) \leftrightarrow \mathbb{Z}_2, \mathbb{Q} \leftrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ .  $\square$

21. [Jan 89 #4; Feb 84 # 2] (a) Find  $Gal(x^3 - 2|\mathbb{Q})$ . (b) Find  $f(x) \in \mathbb{Q}[x]$  with  $Gal(f|\mathbb{Q}) = \mathbb{Z}_2 \times S_3$ .

*Proof.* (a)  $x^3 - 2$  is irreducible over  $\mathbb{Q}$  because it has no rational roots.  $x^3 - 2$  has roots  $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ , where  $\omega$  is a primitive cube root of unity. Then  $x^3 - 2$  splits over  $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ . Note  $\omega \notin \mathbb{Q}(\sqrt[3]{2})$ , and  $\omega$  satisfies the polynomial  $(x^3 - 1)(x - 1) = x^2 + x + 1$ . Then  $[E : \mathbb{Q}] = 6$ , and  $Gal(x^3 - 2|\mathbb{Q})$  is isomorphic to one of  $S_3$  or  $\mathbb{Z}_6$ . But  $\mathbb{Q}(\sqrt[3]{2})$  is not a normal field extension, so  $Gal(x^3 - 2|\mathbb{Q})$  contains a non-normal subgroup, so  $Gal(x^3 - 2|\mathbb{Q}) \cong S_3$ . (b) Let  $f = (x^3 - 2)(x^2 - 5)$ . Then if  $f$  splits over  $E = \mathbb{Q}(\omega, \sqrt[3]{2}, \sqrt{5})$ .  $[E : \mathbb{Q}] = 12$  ( $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{5})$  because 3 does not divide 2,  $\omega \notin \mathbb{Q}(\sqrt[3]{2}, \sqrt{5})$ ),  $Gal(f|\mathbb{Q}) \cong \mathbb{Z}_2 \times S_3$  since  $\sigma : \sqrt{5} \mapsto -\sqrt{5}$  is of order 2 and commutes with  $Gal(x^3 - 2|\mathbb{Q})$ .  $\square$

22. [Jan 00 #8] Let  $\zeta$  be a primitive 3rd root of unity,  $K = \mathbb{Q}(\zeta)$ , and  $L = K(\sqrt[3]{2})$ . (a) Show that  $L|K$  is a Galois extension, and determine its Galois group  $G = Gal(L|K)$ . (b) Considering  $L$  as a vector space over  $K$ , determine all  $K$ -linear functionals  $f : L \rightarrow K$  which are  $G$ -invariant (i.e.  $f(\sigma(a)) = f(a)$  for all  $\sigma \in G$  and all  $a \in L$ ).

*Proof.* (a)  $L$  is the splitting field of  $x^3 - 2$  over  $K$ , hence  $L|K$  is Galois.  $[L : K] = 3$ . Conclude  $Gal(L|K) \cong \mathbb{Z}_3$ .

(b) A  $K$ -basis for  $L$  is  $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$ . Now there is a  $\sigma \in Gal(L|K)$  such that  $\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}$ . Then  $\sigma(\omega\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$ . So if  $f$  is  $G$ -invariant  $K$ -linear functional on  $L$ ,  $f(\sqrt[3]{2}) = f(\omega\sqrt[3]{2}) = f(\omega^2\sqrt[3]{2})$ , i.e.  $f(\sqrt[3]{2}) = \omega f(\sqrt[3]{2}) = \omega^2 f(\sqrt[3]{2})$ . If  $f(\sqrt[3]{2}) \neq 0$ , then  $1 = \omega = \omega^2$ , which cannot happen, so  $f(\sqrt[3]{2}) = 0$ . Now  $\sigma((\sqrt[3]{2})^2) = \omega^2(\sqrt[3]{2})^2$ , and  $\sigma(\omega^2(\sqrt[3]{2})^2) = \omega^2 \cdot \omega^2(\sqrt[3]{2})^2 = \omega(\sqrt[3]{2})^2$ . So  $f((\sqrt[3]{2})^2) = f(\omega(\sqrt[3]{2})^2) = f(\omega^2(\sqrt[3]{2})^2)$ , i.e.  $f((\sqrt[3]{2})^2) = \omega f((\sqrt[3]{2})^2) = \omega^2 f((\sqrt[3]{2})^2)$ . As before, we must have  $f((\sqrt[3]{2})^2) = 0$ . So if  $a, b, c \in K$ ,  $f(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) = af(1)$ .  $\square$

24. [Jan 00 #7] Suppose that  $f$  is an irreducible polynomial of degree  $n$  with rational coefficients. Let  $K$  be a splitting field for  $f$  over the rationals  $\mathbb{Q}$ , and let  $r_1, \dots, r_n$  be the roots of  $f$  in  $K$ , with  $a = \prod_{i < j} (r_i - r_j)$ . (a) Show that the roots of  $f$  are distinct. (b) If the product  $a$  is not rational, show the Galois group  $Gal(K|\mathbb{Q})$  contains an element which

yields an odd permutation of the roots. (c) If the product  $a$  is not rational, *show* that  $K$  contains at least one quadratic subfield.

*Proof.* (a)  $\text{char } \mathbb{Q} = 0$  implies that all irreducible polynomials in  $\mathbb{Q}[x]$  are separable.

(b) If  $a \notin \mathbb{Q}$  then there is a  $\sigma \in \text{Gal}(K|\mathbb{Q})$  such that  $\sigma(a) \neq a$ . Note  $\sigma(a) = \text{sgn}(\sigma)a$ . Then  $\sigma(a) \neq a$  implies  $\text{sgn}(\sigma) = -1$ , i.e.  $\sigma$  is odd.

(c)  $a^2 = \prod_{i < j} (r_i - r_j)^2$ . Note  $\sigma(a^2) = a^2$  for every  $\sigma \in \text{Gal}(K|\mathbb{Q})$ . Then  $a^2 \in \mathbb{Q}$  so  $\mathbb{Q}(a)$  is a quadratic subfield of  $K$ .  $\square$

25. [Aug 01 #8] Find the Galois group of  $f(x) = x^{13} - 1$  over the rationals  $\mathbb{Q}$  (i.e.  $\text{Gal}(K|\mathbb{Q})$  for the splitting field of  $f(x)$  over  $\mathbb{Q}$ ).

*Proof.* Note that  $x^{13} - 1 = (x - 1)(x^{12} + x^{11} + \cdots + x + 1)$ , and  $f = x^{12} + \cdots + x + 1$  is irreducible over  $\mathbb{Q}$  ( $f(x + 1)$  is Eisenstein with  $p = 13$ ). Let  $\zeta$  be a primitive 13th root of unity. Then  $x^{13} - 1$  splits over  $\mathbb{Q}(\zeta)$  and  $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 12$ . Now  $\sigma \in G(\mathbb{Q}(\zeta)|\mathbb{Q})$  is uniquely determined by  $\sigma(\zeta)$ , and  $\sigma(\zeta) = \zeta^n$  for some  $1 \leq n \leq 12$ . Moreover, for each  $1 \leq n \leq 12$  there is a  $\sigma_n \in G(\mathbb{Q}(\zeta)|\mathbb{Q})$  such that  $\sigma_n(\zeta) = \zeta^n$  (because  $\zeta^n$  is a primitive 13th root of unity for each  $1 \leq n \leq 12$ ). Hence the map  $\varphi : \mathbb{Z}_{12} \rightarrow G(\mathbb{Q}(\zeta)|\mathbb{Q})$  given by  $\varphi(n) = \sigma_n$  is a bijection. Also  $\sigma_{nm}(\zeta) = \zeta^{nm} = (\zeta^m)^n = \sigma_n(\sigma_m(\zeta))$ , so  $\varphi(nm) = \varphi(n)\varphi(m)$ . Then  $\varphi$  is an isomorphism, and  $G(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong \mathbb{Z}_{12}$ .  $\square$

26. [Aug 03 #5] Choose your favorite one, denoted by  $G$ , between the Klein four group (i.e.  $\mathbb{Z}_2 \times \mathbb{Z}_2$ ) and the dihedral group  $D_8$  of order 8. Provide an example of an irreducible degree 4 polynomial whose Galois group over  $\mathbb{Q}$  is isomorphic to  $G$ . Show your work.

*Proof.* (i) Recall  $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(i + \sqrt{2})$ , and  $\text{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ . So  $\deg \mu_{\sqrt{2}+i|\mathbb{Q}} = 4$ . but  $\sqrt{2} + i$  satisfies  $x^4 - 2x^2 + 9$ , so  $\mu_{\sqrt{2}+i|\mathbb{Q}} = x^4 - 2x^2 + 9$ . Then  $\text{Gal}(x^4 - 2x^2 + 9|\mathbb{Q}) = \text{Gal}(\mathbb{Q}(\sqrt{2} + i)|\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ .

(ii) Let  $g(x) = x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x + i\sqrt[4]{2})(x - i\sqrt[4]{2})$ . Then  $g$  has splitting field  $L = \mathbb{Q}(\sqrt[4]{2}, i)$ ,  $[L : \mathbb{Q}] = 8$ . There are  $\sigma, \tau \in \text{Gal}(L|\mathbb{Q})$  given by  $\sigma : \sqrt[4]{2} \mapsto i\sqrt[4]{2}, i \mapsto i$ ,  $\tau : \sqrt[4]{2} \mapsto \sqrt[4]{2}, i \mapsto -i$ . Then  $\text{ord}(\sigma) = 4$ ,  $\text{ord}(\tau) = 2$ , and  $\tau\sigma\tau(i\sqrt[4]{2}) = \tau\sigma(-i\sqrt[4]{2}) = \tau(\sqrt[4]{2}) = \sqrt[4]{2}$ ,  $\tau\sigma\tau(i) = \tau(\sigma(-i)) = \tau(-i) = i$ . So  $\tau\sigma\tau = \sigma^{-1}$ . Now  $\langle \sigma \rangle \rtimes \langle \tau \rangle$ , where  $\tau\sigma\tau = \sigma^{-1}$ , is a subgroup of  $G(L|\mathbb{Q})$  of order 8, so it must be the whole group, and is isomorphic to  $D_8$ .  $\square$

# Chapter 5

## Multilinear Algebra

### 5.1 Dual spaces and bilinear forms

1. [Aug 94 #5] If  $f(x, y)$  is an alternating bilinear form on a 25-dimensional real vector space, and  $A$  is its matrix with respect to some basis, show that  $\deg(A)^{25} = 0$ .

*Proof.* Let  $\{e_1, \dots, e_{25}\}$  be a basis for  $V$ . Then  $f$  is represented by the matrix  $A = (f(e_i, e_j))$ . Now  $A^T = (f(e_j, e_i)) = (-f(e_i, e_j)) = -A$ . Then  $\det(A) = \det(A^T) = \det(-A) = (-1)^{25} \det(A) = -\det(A)$ , so  $\det(A) = 0$ .  $\square$

2. [Jan 97 #7] Let  $V$  be a finite-dimensional vector space over a field  $F$ , and let  $\lambda$  and  $\mu$  be two linear functionals on  $V$ . Define  $B(x, y) = \lambda(x)\mu(y) - \lambda(y)\mu(x)$  for  $x, y \in V$ . Show that  $B$  is an alternating bilinear form on  $V$ , and determine the possible values for its rank.

*Proof.* Determining the possible values for the rank of  $B$ : Choose a basis  $\{e_1, \dots, e_n\}$  of  $V$ . Then  $B$  corresponds to the matrix  $(B(e_i, e_j)) = \underbrace{(\lambda(e_i)\mu(e_j))}_A - \underbrace{(\lambda(e_j)\mu(e_i))}_C$ . Each of  $A$  and  $C$  has rank no larger than 1, so the rank of  $B$  is either 0 or 2.  $\square$

3. [Aug 95 #7] Show that every element of

$$SO_5(\mathbb{R}) = \{A \in GL_5(\mathbb{R}) \mid (Ax, Ay) = (x, y) \text{ and } \det(A) = 1\}$$

[where  $(x, y) = x \cdot y = x^t y$  is the usual dot product on  $\mathbb{R}^5$ ] has a nonzero fixed point  $Ax = x \neq 0$ .

*Proof.* Show each  $A \in SO_5(\mathbb{R})$  has an eigenvalue of 1. Since  $n = 5$ , each  $A \in SO_5(\mathbb{R})$  has at least one real eigenvalue. If  $x$  is an eigenvector for the real eigenvalue  $\lambda \in \mathbb{R}$ ,  $(Ax, Ax) = (x, x)$ , i.e.  $(\lambda x, \lambda x) = (x, x)$ , so  $\lambda^2(x, x) = (x, x)$ . Thus,  $\lambda = \pm 1$ . Product of

complex conjugate eigenvalues is positive, and product of all eigenvalues is 1, so  $-1$  can only appear as an eigenvalue with even multiplicity. Conclude that 1 must be an eigenvalue. Then there is an  $x \neq 0$  such that  $Ax = x$ .  $\square$

4. [Aug 95 Comprehensive #10] It is known that the space  $M_n(\mathbb{R})$  of  $n \times n$  real matrices is a real inner product space with inner product given by  $\langle A, B \rangle = \text{tr}(AB^T)$ , where  $B^T$  denotes the transpose of the matrix  $B$ . Let  $P$  be an invertible matrix and  $T$  the linear operator on  $M_n(\mathbb{R})$  defined by  $T(A) = P^T AP$ . Denote the adjoint of  $T$  relative to this inner product by  $T^*$ . Prove that  $T^*(A) = PAP^T$  for all  $A$ , and find necessary and sufficient conditions on the matrix  $P$  so that  $T = T^*$ . Justify your answer.

*Proof.* Have  $T^*$  defined by  $\langle TA, B \rangle = \langle A, T^*B \rangle$ , i.e.  $\text{tr}(A(T^*B)^T) = \text{tr}(P^T APB^T)$ . Now  $\text{tr}(P^T APB^T) = \text{tr}(APB^T P^T) = \text{tr}(A(PBP^T)^T) = \langle A, PBP^T \rangle$ . Conclude that  $T^*(A) = PAP^T$ . Now  $T = T^*$  iff  $PAP^T = P^T AP$  for every  $A \in M_n(\mathbb{R})$ . Now  $PAP^T = P^T AP$  for every  $A \in M_n(\mathbb{R})$  implies that  $P(P^{-1}A)P^T = P^T(P^{-1}A)P$  for every  $A \in M_n(\mathbb{R})$ , so  $AP^T = (P^T P^{-1})AP$ , i.e.  $A(P^T A^{-1}) = (P^T P^{-1})A$  for every  $A \in M_n(\mathbb{R})$ , and then  $P^T P^{-1} = rI_n$  for some  $r \in \mathbb{R}$ . Then  $P^T = rP$  for some  $r \in \mathbb{R}$ . If  $P^T = (rI)P$  for some  $r \in \mathbb{R}$ , then  $PAP^T = PA(rI)P = P(rI)AP = P^T AP$  for every  $A \in M_n(\mathbb{R})$ .  $\square$

6. [Aug 03 #6] Let  $B$  be a symmetric bilinear form on a finite-dimensional vector space  $V$  over a field  $F$ . For a subspace  $W \subseteq V$ , we define the annihilator subspace of  $W$  in  $V$ :  $W^\perp = \{x \in V \mid B(x, w) = 0 \text{ for every } w \in W\}$ . Assume further that  $B$  is nondegenerate, that is  $V^\perp = \{0\}$ . Show that: (a) there is a natural isomorphism of vector spaces from  $V/W^\perp$  to the dual space  $W^*$  of  $W$ ; (b)  $\dim W^\perp = \dim V - \dim W$ ; (c)  $(W^\perp)^\perp = W$ .

*Proof.* (a) Define  $\psi : V \rightarrow V^*$  by  $\psi(v) = B(v, \cdot)$ . For  $u, v \in V, r \in F$ ,  $\psi(u+v) = B(u+v, \cdot) = B(u, \cdot) + B(v, \cdot) = \psi(u) + \psi(v)$ , and  $\psi(rv) = B(rv, \cdot) = rB(v, \cdot) = r\psi(v)$ . So  $\psi$  is a vector space homomorphism. Since  $V^\perp = \{0\}$ ,  $\psi$  is injective. Then  $\dim_F(V) = \dim_F(\psi(V))$ . But  $\dim_F(V) < \infty$  implies that  $\dim_F(V^*) = \dim_F(V)$ . Now  $\psi(V) \subseteq V^*$  and  $\dim_F(\psi(V)) = \dim_F(V^*)$ , so  $\psi(V) = V^*$ , and  $\psi$  is an isomorphism. The map  $\Phi : V^* \rightarrow W^*$  given by  $\Phi(f) = f|_W$  is a surjective homomorphism of vector spaces. Consider the composition  $\Phi \circ \psi$ , which has kernel equal to  $W^\perp$ . Then  $\Phi \circ \psi : V/W^\perp \rightarrow W^*$  is an isomorphism.  $\square$

7. [Sep 83 #8] If  $E|\mathbb{Q}$  is Galois and  $B(x, y) = \text{tr}_{E|\mathbb{Q}}(xy)$  (you may assume this is a nondegenerate bilinear form on  $E \times E$  to  $\mathbb{Q}$ ), find the adjoints  $\sigma^*$  of the elements  $\sigma$  of the Galois group  $G(E|\mathbb{Q})$  with respect to the bilinear form  $B$ .

*Proof.*  $B(x, y) = \text{tr}_{E|\mathbb{Q}}(xy) = \sum_{\tau \in G} \tau(xy) = \sum_{\tau \in G} \tau(x)\tau(y)$ . Given  $\sigma \in G = \text{Gal}(E|\mathbb{Q})$ ,  $\sigma^*$  is defined by the relationship  $B(\sigma(x), y) = B(x, \sigma^*(y))$ , i.e

$$\sum_{\tau \in G} \tau\sigma(x)\tau(y) = \sum_{\tau \in G} \tau(x)\tau(\sigma^*(y))$$

But  $\sum_{\tau \in G} \tau\sigma(x)\tau(y) = \sum_{\tau \in G} (\tau\sigma^{-1})(\sigma(x))(\tau\sigma^{-1})(y) = \sum_{\tau \in G} \tau(x)(\tau\sigma^{-1})(y)$ . Then  $\sigma^* = \sigma^{-1}$ .  $\square$

## 5.2 Tensor Products

1. [Aug 03 #4] (a) Determine the following tensor products and explain your answers: (i)  $\mathbb{R} \otimes_{\mathbb{Z}} \mathbb{Z}_{2003}$ ; (ii)  $\mathbb{Q}[x]/(x^2 + 1) \otimes_{\mathbb{Q}[x]} \mathbb{Q}[x]/(x^2 + 2)$ . (b) Let  $V$  and  $W$  be finite-dimensional vector spaces over a field  $F$ , and  $\{v_1, \dots, v_n\}$  be a basis of  $V$ . Prove that if

$$v_1 \otimes w_1 + \dots + v_n \otimes w_n = 0$$

in  $V \otimes_F W$  for  $w_1, \dots, w_n \in W$ , then  $w_1 = w_2 = \dots = w_n = 0$ .

*Proof.* (a) (i) Suppose  $a \in \mathbb{R}$  and  $\bar{b} \in \mathbb{Z}_{2003}$ . Then  $a \otimes_{\mathbb{Z}} \bar{b} = 2003 \cdot \frac{a}{2003} \otimes_{\mathbb{Z}} \bar{b} = \frac{a}{2003} \otimes_{\mathbb{Z}} 2003\bar{b} = \frac{1}{2003} \otimes_{\mathbb{Z}} 0 = 0$ . Therefore,  $\mathbb{R} \otimes_{\mathbb{Z}} \mathbb{Z}_{2003} = \{0\}$ . (ii)  $\mathbb{Q}[x]/(x^2 + 1) \otimes_{\mathbb{Q}[x]} \mathbb{Q}[x]/(x^2 + 2) \cong \mathbb{Q}[x]/(x^2 + 1, x^2 + 2) = \mathbb{Q}[x]/(1) = \{0\}$ .

(b) Let  $\varphi : V \times W \rightarrow \bigoplus_{i=1}^n W$  be given by  $\varphi(\sum r_i v_i, w) = (r_i w)_{i=1}^n$ . Then  $\varphi$  is  $F$ -bilinear, so there is an  $F$ -linear map  $\Phi : V \otimes_F W \rightarrow \bigoplus_{i=1}^n W$  such that  $\Phi(\sum r_i v_i \otimes w) = (r_i w)_{i=1}^n$ . Now  $\sum v_i \otimes w_i = 0$  implies  $0 = \Phi(0) = \Phi(\sum v_i \otimes w_i) = (w_i)_{i=1}^n$ . Then  $w_i = 0$  for every  $i$ .  $\square$

3. [May 04 Final #7] Prove or disprove: (a)  $\mathbb{Q}(\sqrt{10}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{10})$  is isomorphic to  $\mathbb{Q}(\sqrt{10})$  as a  $\mathbb{Q}$ -vector space. (b)  $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$  is isomorphic to  $\mathbb{Q}$  as a  $\mathbb{Z}$ -module.

*Proof.* (a)  $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{10}) = 2$ . Then  $\dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt{10}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{10})) = [\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{10})]^2 = 4$ , so the statement is false.

(b) The map  $\varphi : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$  given by  $(a, b) \mapsto ab$  is  $\mathbb{Z}$ -bilinear, so there is a  $\mathbb{Z}$ -linear map  $\Phi : \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow \mathbb{Q}$  given by  $a \otimes b \mapsto ab$ . Let  $\psi : \mathbb{Q} \rightarrow \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$  be given by  $\psi(a) = 1 \otimes a$ . Note, given  $m/n, r/s \in \mathbb{Q}$ ,  $\frac{m}{n} \otimes_{\mathbb{Z}} \frac{r}{s} = \frac{m}{n} \otimes_{\mathbb{Z}} n \frac{r}{sn} = m \otimes_{\mathbb{Z}} \frac{r}{sn} = 1 \otimes \frac{rm}{sn}$ . Now  $\psi$  is a  $\mathbb{Z}$ -linear map. Have  $\psi \circ \Phi(a \otimes b) = \psi(ab) = 1 \otimes ab = a \otimes b$ , by the remark above, and  $\Phi \circ \psi(a) = \Phi(1 \otimes a) = a$ . So  $\psi, \Phi$  are inverses on simple tensors, so they are inverse isomorphisms, and  $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$ .  $\square$

4. [Aug 04 #8] Let  $K$  be a field,  $V$  a finite-dimensional vector space over  $K$ , and  $v, w$  two non-zero vectors in  $V$ . Show that  $v \otimes w = w \otimes v$  in  $V \otimes_K V$  if and *only if* there exists a  $c \in K^*$  such that  $w = cv$ .

*Proof.* If  $w = cv$  for some  $c \in K^*$ ,  $v \otimes w = v \otimes cv = cv \otimes v = w \otimes v$ . Suppose  $w \neq cv$  for every  $c \in K^*$ . Then  $v, w$  are  $K$ -linearly independent. Then there is a  $k$ -basis  $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$  of  $V$  with  $v_1 = v$  and  $v_2 = v - w \neq 0$ . Now  $0 = v \otimes w - w \otimes v = (v \otimes w) - (v \otimes v) + (v \otimes v) - (w \otimes v) = v \otimes (w - v) + (v - w) \otimes v$ . Then  $w - v = 0, v = 0$ , i.e.  $v = w = 0$ , contradiction. Conclude  $w = cv$  for some  $c \in K^*$ .  $\square$

6. Let  $I$  and  $J$  be ideals of  $R$ . Show that  $R/I \otimes_R R/J$  is isomorphic (as  $R$ -modules) to  $R/(I + J)$ .

*Proof.* Let  $\varphi : R/I \times R/J \rightarrow R/(I + J)$  be given by  $(a + I, b + J) \mapsto ab + (I + J)$ . This is a well-defined map since if  $i \in I$  and  $j \in J$ , then  $(a + i + I, b + j + J) \mapsto (a + i)(b + j) + (I + J) = ab + aj + bi + ij + (I + J) = ab + (I + J)$ . Moreover,  $\varphi$  is  $R$ -bilinear. Then there is an  $R$ -linear map  $\Phi : R/I \otimes_R R/J \rightarrow R/(I + J)$  such that  $(a + I) \otimes_R (b + J) \mapsto ab + (I + J)$ . Let  $\psi : R \rightarrow R/I \otimes_R R/J$  be given by  $r \mapsto (1 + I) \otimes_R (r + J)$ . If  $i \in I, j \in J$ , then  $\psi(i + j) = (1 + I) \otimes (i + j + I) = (1 + I) \otimes (i + J) = i(1 + I) \otimes (1 + J) = (i + I) \otimes (1 + J) = (0 + I) \otimes (1 + J) = 0$ . So there is a map  $\bar{\psi} : R/(I + J) \rightarrow R/I \otimes_R R/J$ , given by  $a + (I + J) \mapsto (1 + I) \otimes_R (a + J)$ . Now  $\bar{\psi} \circ \Phi = id$  and  $\Phi \circ \bar{\psi} = id$  on simple tensors, so we conclude the two  $R$ -modules are isomorphic.  $\square$