Final Exam Practice

Math 511a

1 Groups

1. Determine all the homomorphisms from S_3 to A_4.

   Solution 1 *All homomorphisms have kernels. The only normal subgroups of* S_3 *are* $1, A_3, S_3$. *Thus the image of* S_3 *can go to a subgroup of* A_4 *of size* $6, 2, 1$. *But there is no subgroup of* A_4 *of order* 6. *Thus we can only map by the trivial map or to a subgroup of size* 2. *If* $|H| = 2$ *with* $H \leq A_4$ *then we map the elements of* S_3 *according to whether they are odd or even. We map into a subgroup of* A_4 *such as* $\langle (12)(34) \rangle$ *by mapping even permutations in* S_3 *to the identity and odd ones to* $(12)(34)$.

2. Let G be a group of order pqr, where p, q, r are primes and $p > q > r$. Show that G is solvable.

   Solution 2 *The number of Sylow* p*-subgroups is* $1 + kp$, *where* $1 + kp$ *divides* qr. *Suppose* $k \neq 0$. *Since* $p > q > r$, $1 + kp = qr$. *The number of Sylow* q*-subgroups is* $1 + k'q$, *where* $1 + k'q$ *divides* pr. *Suppose* $k' \neq 0$. *Since* $q > r$, *either* $1 + k'q = p$ *or* pr. *In either case,* $1 + k'q \geq p$. *The number of Sylow* r*-subgroups is* $1 + k''r$, *where* $1 + k''r$ *divides* pq. *Suppose* $k'' \neq 0$. *Then either* $1 + k''r = q$ *or* p *or* pq. *Hence, in either case,* $1 + k''r \geq q$. *Thus,* G *has* $qr(p-1)$ *elements of order* p, *at least* $p(q-1)$ *elements of order* q, *and at least* $q(r-1)$ *elements of order* r. *Since* G *has* pqr *elements,* $pqr \geq rq(p-1) + p(q-1) + q(r-1) + 1$. *This implies that* $0 \geq pq - p - q + 1$ *or* $0 \geq (p-1)(q-1)$. *Therefore,* $(p-1)(q-1) = 0$, *which implies that either* $p = 1$ *or* $q = 1$, *a contradiction. Thus either* $k = 0$ *or* $k' = 0$ *or* $k'' = 0$. *WLOG, suppose* $k = 0$. *Then* G *has a unique Sylow* p*-subgroup, say,* H. *Now* H *is a normal subgroup of* G *and* G/H *is of order* qr. *By a previous result this semester we know that* G/H *is solvable. Since* H *is of order* p, H *is solvable. Hence, by Theorem 5.4 (Grove),* G *is Solvable.*

3. Let G be the group of all $n \times n$ invertible matrices over $\mathbb{R}$, $n \geq 3$. Show that G is not solvable.

   Solution 3 *Let* E_{ij} *be the* $n \times n$ *elementary matrix whose* ij^{th} *entry is* 1 *and all else are zero. Then*

   $$E_{ij}E_{rs} = \left\{ \begin{array}{c} E_{is}, j = r \\ 0, j \neq r \end{array} \right\}.$$

Now for the identity matrix I and for $i \neq j$, $I+E_{ij} \in G$ and $(I+E_{ij})^{-1} = 1-E_{ij}$. Let T be the subgroup generated by $\{I+E_{ij} : i \neq j\}$. Since $n \geq 3$, we can find an integer k such that $1 \leq i \neq k \neq j \leq n$. Now

$$\begin{aligned}(I+E_{ik})(I+E_{kj})(I+E_{ik})^{-1}(I+E_{kj})^{-1} = \\ (I+E_{ik})(I+E_{kj})(I-E_{ik})(I-E_{kj}) = \\ (I+E_{kj}+E_{ik}+E_{ij})(1-E_{kj}-E_{ik}+E_{ij}) = \\ (I+E_{ij}).\end{aligned}$$

Therefore, $(I+E_{ij}) \in T'$, proving that $T \subseteq T'$. As a result, $T' = T$. Thus, T is not solvable and so G is not solvable.

4. Find all the composition series of the group $\mathbb{Z}/42\mathbb{Z}$. Verify that they are equivalent.

Solution 4 $\mathbb{Z}/42\mathbb{Z} \supset 2\mathbb{Z}/42\mathbb{Z} \supset 14\mathbb{Z}/42\mathbb{Z} \supset 42\mathbb{Z}/42\mathbb{Z}$

$\mathbb{Z}/42\mathbb{Z} \supset 2\mathbb{Z}/42\mathbb{Z} \supset 6\mathbb{Z}/42\mathbb{Z} \supset 42\mathbb{Z}/42\mathbb{Z}$

$\mathbb{Z}/42\mathbb{Z} \supset 3\mathbb{Z}/42\mathbb{Z} \supset 6\mathbb{Z}/42\mathbb{Z} \supset 42\mathbb{Z}/42\mathbb{Z}$

$\mathbb{Z}/42\mathbb{Z} \supset 3\mathbb{Z}/42\mathbb{Z} \supset 21\mathbb{Z}/42\mathbb{Z} \supset 42\mathbb{Z}/42\mathbb{Z}$

$\mathbb{Z}/42\mathbb{Z} \supset 7\mathbb{Z}/42\mathbb{Z} \supset 14\mathbb{Z}/42\mathbb{Z} \supset 42\mathbb{Z}/42\mathbb{Z}$

$\mathbb{Z}/42\mathbb{Z} \supset 7\mathbb{Z}/42\mathbb{Z} \supset 21\mathbb{Z}/42\mathbb{Z} \supset 42\mathbb{Z}/42\mathbb{Z}$

Each of the above six composition series has three factors. These factors are nothing but the groups $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_7$. Hence, all these composition series are equivalent.

5. Find a central series $G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n$ in D_4 such that $G_0 = \{1\}$ and $G_n = D_4$.

Solution 5 *$D_4 = \langle a, b : a^4 = b^2 = 1, ba = a^3b\rangle$. Now*

$$\{1\} = G_0 \subseteq G_1 = \{1, a^2\} \subseteq G_2 = \{1, a, a^2, a^3\} \subseteq G_3 = D_4$$

is a normal series in D_4. Since $|D_4/G_1| = 4$ and $|D_4/G_2| = 2$, it follows that D_4/G_1 and D_4/G_2 are abelian groups. Thus, $G_2/G_1 \subseteq D_4/G_1 = Z(D_4/G_1)$ and $D_4/G_2 \subseteq Z(D_4/G_2)$. Since $Z(D_4) = \{1, a^2\} = G_1$, it follows that $G_1/G_0 \subseteq Z(D_4/G_0)$. Hence $\{1\} \subseteq \{1, a^2\} \subseteq \{1, a, a^2, a^3\} \subseteq D_4$ is a central series.

6. Give an example of a group G such that G is not nilpotent, but G contains a normal subgroup H such that H and G/H are nilpotent.

Solution 6 *The symmetric group S_3 is not nilpotent as it is centerless. Now A_3 is nilpotent as it is abelian and it is normal in S_3. Also, $|S_3/A_3| = 2$ and so is abelian and thus nilpotent.*

7. List all normal subgroups of $A_5 \times A_5$.

   Solution 7 1×1, $A_5 \times 1$, $1 \times A_5$, $A_5 \times A_5$

8. Suppose S is a set and the symmetric group S_4 acts transitively on S. Determine all possibilities for $|S|$.

   Solution 8 *There is a bijection between all possible actions of a group G on a set A with the possible homomorphisms from G to S_A. By the Orbit stabilizer theorem we know that $|\mathrm{Orb}_G(s)| = [G : \mathrm{Stab}_G(s)]$. For a transitive action, the size of the entire set occurs as the index of a subgroup of G. This gives us a list of possible set sizes. The most canonical map to use is $G \times G/H \to G/H$ by $g_1 \times g_2H \to g_1g_2H$ and this is a well-defined action and we can identify each of the elements of our given set with one of the cosets. This is a transitive action as if we want to move g_2H to g_3H we just multiply by $g_3g_2^{-1}$ as our g_1. So we must find all possible subgroups of S_4. They have size $1, 2, 3, 4, 6, 8, 12, 24$. So all divisors of 24 occur as possible sizes of S.*

9. Show that a group of order 48 must have a normal subgroup of order a power of 2.

   Solution 9 *$|G| = 2^4 \cdot 3$. So there are 1 or 3 2-sylow subgroups of order 16. If there is one it must be normal and so we are done. If not there are 3, call them A, B, C. The order of the subset AB is $|AB| = \dfrac{|A|\,|B|}{|A \cap B|} \leq 48 = |G|$. So $\dfrac{16 \cdot 16}{|A \cap B|} \leq 48$ where $|A \cap B|$ divides $|G|$ as it is a subgroup. The only possibilities are 16 or 8. But we know it is not 16 as A and B are distinct. So it must be 8. So $A \cap B \lhd A$ and $A \cap B \lhd B$. So $AB \subseteq N_G(A \cap B)$. But $|AB| = 32$ and $N_G(A \cap B) \leq G$ it must have have order 48. Thus $N_G(A \cap B) = G$ and so $A \cap B \lhd G$ and has order $2^3 = 8$.*

10. Let G be the group of real 2×2 matrices of determinant 1, and let H be the subgroup of diagonal matrices.

    (a) Find the normalizer of H in G, $N_G(H)$.

    (b) Find the representatives for the cosets in $N_G(H)$.

    Solution 10 *Did in review session!*

11. Let p be a prime number. Let $\mathbb{F}_p$ be the field of p elements. Let $G = GL_2(\mathbb{F}_p)$ be the 2×2 invertible matrices with entries in $\mathbb{F}_p$. Let G act on the vector space $V = \mathbb{F}_p \times \mathbb{F}_p$ in the usual way (by matrix multiplication).

    (a) Show that G has exactly 2 orbits on V.

(b) Compute the order of the stabilizer of $(1,0)$.

(c) Use part (b) to compute the order of G.

Solution 11 *(a) The element $(0,0) \in V$ composes one orbit; certainly $A0 = 0$ for any matrix A, and if $Ax = 0$ for an invertible matrix A, then $x = A^{-1}0 = 0$. We shall show now that the rest of V composes the second orbit. To establish this, we must show, given any nonzero $x, y \in V$, the existence of an invertible matrix A such that $Ax = y$. If x, y are linearly dependent, then $\lambda x = y$ and so $A = \lambda I$. Use linear algebra and there is always a solution to $Ax = y$ if A is invertible.*

(b) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ implies $a = 1$ and $c = 0$ and so for the matrix to be invertible we have $p-1$ choices for d and p for b so there are $p(p-1)$ total. Thus $|\mathrm{Stab}_G(1,0)| = p^2 - p$.

(c) The index of the stabilizer of $(1,0)$ is the size of the orbit of $(1,0)$; the order of V is p^2 and so $[G : \mathrm{Stab}] = p^2 - 1$. Thus $|G| = \left(p^2 - 1\right)\left(p^2 - p\right)$.

12. Either give an example of a finite group having its center of prime index or prove that such a group cannot exist.

Solution 12 *It cannot exist. If it did, then the quotient would be cyclic and thus abelian. Thus the group was abelian (proved earlier this year). If the group is abelian the index is* 1.

13. Suppose p is a prime and G is a finite group. A subgroup K of G is called a normal p-complement if $K \lhd G$ and there is a Sylow p-subgroup P such that $K \cap P = 1$ and $KP = G$. Show that if G has a normal p-complement, then it is unique. Give an example.

Solution 13 *Example: $\mathbb{Z}_{15}$ is the internal direct sum of its cyclic subgroups of order* 3 *and* 5*; call them K and P. Here K is a normal* 3*-complement; certainly K is normal as it is abelian and there is a* 5*-Sylow, namely P, such that $K \cap P = 1$ and $KP = G$.*

Let the p-Sylow subgroup P have order p^k. Since $KP = G$ and $K \cap P = 1$, we must have $|K| = |G|/p^k$. The claim is that K must be the set of elements of G of order not a multiple of p. (This would show K to be unique). Let H denote the set of elements. Since each element of K has order dividing $|G|/p^k$, certainly $K \subseteq H$. Now consider the canonical projection map $G \to G/K$, observing that G/K is a p-group. Under the group homomorphism, the order of the image of an element must divide the order of the original element. But the only possible orders in G/K are $1, p, p^2$ and so on. Hence any element of H gets mapped to an element of order 1*, i.e., it represents the trivial coset of K and thus lies in K. In short, $H \subseteq K$. Combining the results, we have $K = H$ and thus K is unique.*

14. Let H be the subgroup of S_7, the symmetric group of 7 letters, generated by all 3-cycles. Is the permutation (1234) in H? Explain.

    Solution 14 *The 3-cycles generate the alternating subgroup of S_n for $n \geq 3$. Thus H is the alternating group A_7 and does not contain the odd permutation* (1234).

15. Give an example or prove that there does not exist a group of order 5! acting transitively on a set with 9 elements.

    Solution 15 *There does not exist such an action. In any group action, the size of an orbit always equals the index of the stabilizer of a point in that orbit. A transitive action has a single orbit. Thus we have a stabilizer of index* 9; *but this is impossible since* 9 *does not divide* 5!.

16. What are the conjugacy classes of S_3?

    Solution 16 $\{\mathrm{id}\}, \{(12), (23), (13)\}$, *and* $\{(123), (132)\}$

17. Suppose G is a group of order 45 with a normal subgroup P of order 3^2. Show that G is abelian. (Hint: $\mathrm{Aut}(P)$ has order 6 or 24 according to whether P is cyclic or elementary abelian).

    Solution 17 *Recall the quotient $G/C_G(P)$ is isomorphic to a subgroup of* $\mathrm{Aut}(P)$, *where $C_G(P)$ is the centralizer of P.* $\mathrm{Aut}(P)$ *has order* 6 *or* 24. *On the other hand, since the order of P is the square of a prime, P is an abelian group, hence $P \leq C_G(P)$. It follows that $|C_G(P)|$ is divisible by* 9, *which implies that $|G/C_G(P)| = 1$ or* 5. *Together these imply $|G/C_G(P)| = 1$, i.e., $C_G(P) = G$ and $P \leq Z(G)$. Since $G/Z(G)$ is cyclic, G must be an abelian group.*

18. True or false: If G is a nonabelian group then it has abelian subgroups H_α such that $G = \cup_\alpha H_\alpha$ and $\cap_\alpha H_\alpha = 1$.

    Solution 18 *I think false. Take the quaternion group of size* 8.

19. Show that the alternating group A_6 has no subgroup of order 72.

    Solution 19 *Consider the homomorphism from A_6 to S_5. See Grove p.15 for a discussion on the natural action of G on $S = \{xH : x \in G\}$ with H a subgroup of G. An element $x \in G$ is in the kernel of the action if and only if $xyH = yH$. Thus the kernel is $K = \cap\{H^z : z \in G\}$. Then this permutation action of G on S is a homomorphism ϕ from G into $Perm(S)$, which is isomorphisc to S_n. Thus the kernel of the action must be trivial because A_6 is simple. But this is not a faithful action as A_6 is not isomorphic to a subgroup of S_5. Thus we cannot have a subgroup of order* 72.

2 Rings

1. Determine positive integers n such that $\mathbb{Z}_n$ has no nonzero nilpotent elements.

   Solution 20 *The claim is that n is a square free integer, i.e. $n = p_1 \cdots p_k$ where the $p_i's$ are distinct.*

   Suppose that $n = p_1 \cdots p_k$. Let $[a] \in \mathbb{Z}_n$ be nilpotent. Then $a^m = 0$ for some integer m. Hence, n divides a^m and so $p_1 \cdots p_k$ divides a^m. Then $p_i | a^m$ for all $i = 1, ..., k$. Since the $p_i's$ are prime, $p_i | a$ for all $i = 1, 2, ..., k$. Since $p_1, ..., p_k$ are distinct primes, we must have $p_1 \cdots p_k | a$, i.e., $n|a$ and so $a = 0$. This implies that $\mathbb{Z}_n$ has no nonzero nilpotent elements. Conversely, suppose that $\mathbb{Z}_n$ has no nonzero nilpotent elements. Let $n = p_1^{m_1} \cdots p_k^{m_k}$, where the $p_i's$ are distinct primes and $m_i \geq 1$. Let $m = \max\{m_1, ..., m_k\}$. Now $[p_1 p_2 \cdots p_k]^m = p_1^m \cdots p_k^m = 0$ since $n | (p_1^m \cdots p_k^m)$. Also, since $\mathbb{Z}_n$ has no nonzero nilpotent elements, $[p_1 \cdots p_k] = 0$. Hence, $n | (p_1 \cdots p_k)$ and so $(p_1^{m_1} \cdots p_k^{m_k}) | (p_1 \cdots p_k)$. Thus $m_i \leq 1$ for all i. So n is square free.

2. Write the proof if the statement is true; otherwise give a counterexample

   (a) In a ring R, if a and b are idempotent elements, then $a + b$ is an idempotent element.

   (b) In a ring R, if a and b are nilpotent elements, then $a + b$ is nilpotent.

   (c) Every finite ring with 1 is an integral domain.

   (d) There exists a field with seven elements.

   (e) The characteristic of an infinite ring is always 0.

   (f) An element of a ring R which is idempotent, but not a zero divisor, is the identity element of R.

   (g) If a and b are two zero divisors, then $a + b$ is also a zero divisor in a ring R.

   (h) In a finite field F, $a^2 + b^2 = 0$ implies $a = 0$ or $b = 0$ for all $a, b \in F$.

   (i) In a field F, $(a + b)^{-1} = a^{-1} + b^{-1}$ for all nonzero elements such that $a + b \neq 0$.

   (j) There exists a field with six elements.

   Solution 21 *(a) False: think matrices (b) False: matrices (c) False: Z_4 (d) True: $\mathbb{F}_7$ (e) False: $Z_2 \times Z_2 \times \cdots$ (f) True (g) False: matrices E_{11} and E_{22} (h) False: $\mathbb{C}$ (i) False: $(1 + 1)^{-1} \neq 1 + 1$ (j) False: only order p^n.*

3. Let R be a ring such that R has no zero divisors. Show that if every subring of R is an ideal of R, then R is commutative.

Solution 22 *Let* $0 \neq a \in R$. *Then* $C(a) = \{x \in R : xa = ax\}$ *is a subring of* R *and hence an ideal of* R, *Thus,* $ra \in C(a)$ *for all* $r \in R$. *Let* $r \in R$. *Now* $ara = ra^2$ *implies that* $(ar - ra)\, a = 0$. *Since* R *has no zero divisors and* $a \neq 0$, $ar - ra = 0$ *and so* $ar = ra$. *Hence,* a *is in the center of* R. *Since* a *is arbitrary,* R *is commutative.*

4. Prove or give counterexample

   (a) There exist only two homomorphisms from the ring of integers into itself.

   (b) The mapping $f : Z \to Z$ defined by $f(n) = 3n$ is a group homomorphism, but not a ring homomorphism.

   (c) The only isomorphism of a ring R onto itself is the identity mapping of R.

   (d) Let R be a ring with 1. Let $f : R \to S$ be a ring homomorphism. Then $f(1)$ is the identity element of S.

   (e) A nonzero homomorphism from a field into a ring with more than one element is a monomorphism.

   (f) Every nontrivial homomorphic image of an integral domain is an integral domain.

   Solution 23 *(a) True:* $f(1) = 1$ *or* 0. *(b) True: Check group hom and see* 1. *(c) False: Take* $\mathbb{C}$ *and conjugation. (d) False: the zero map. This is true only if the map is surjective I believe (e) True: What about the kernel? (f) False: Map* $Z \to Z_6$.

5. An idempotent e of a ring R is called a central idempotent if $e \in C(R)$, the center of the ring and $e^2 = e$. Let R be a ring with 1 and e be a central idempotent in R. Show that

   (a) $1 - e$ is a central idempotent in R;

   (b) eR and $(1 - e)\, R$ are ideals of R;

   (c) $R = eR \oplus (1 - e)\, R$

   Solution 24 *(a)* $(1 - e)(1 - e) = 1 - e - e + e^2 = 1 - e - e + e = 1 - e$. *Also, for all* $a \in R$, $a(1 - e) = a - ae = a - ea = (1 - e)\, a$. *Hence* $1 - e$ *is a central idempotent.*

   (b) Now eR *is a right ideal of* R. *Let* $a \in R$. *Then* $a(eR) = (ae)\, R = (ea)\, R$ *(since* $e \in C(R)) = e(aR) \subseteq eR$. *Hence,* eR *is also a left ideal. Thus,* eR *is an ideal of* R. *Similarly,* $(1 - e)\, R$ *is an ideal of* R.

   (c) Let $a \in R$. *Then* $a = ea + a - ea = ea + (1 - e)\, a \in eR + (1 - e)\, R$. *Hence,* $R = eR + (1 - e)\, R$. *Suppose* $b \in eR \cap (1 - e)\, R$. *Then there exist* $c, d \in R$ *such that* $b = ec = (1 - e)\, d$. *Hence* $eb = e^2 c = ec = b$ *and* $eb = e(1 - e)\, d = \left(e - e^2\right) d = (e - e)\, d = 0$. *Thus,* $b = 0$. *So the intersection is trivial and we have our result.*

6. Let R be a commutative ring with 1 and $f(x) = a_0 + a_1x + ... + a_nx^n \in R[x]$. If a_0 is a unit and $a_1, a_2, ..., a_n$ are nilpotent elements, prove that $f(x)$ is invertible.

   Solution 25 *We prove this result by induction on* $n = \deg f(x)$. *If* $n = 0$, *then* $f(x) = a_0$ *and* a_0 *is a unit so* $f(x)$ *is invertible. Assume the result is true for all polynomials of the above form and degree* $< n$. *Suppose now* $f(x) = a_0 + a_1x + ... + a_nx^n \in R[x]$ *such that* a_0 *is a unit and* $a_1, ..., a_n$ *are nilpotent and* $\deg f(x) = n$. *Let* $g(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1}$. *Note that* $\deg g(x) < n$. *Hence, by the induction hypothesis,* $g(x)$ *is invertible. Since* a_n *is nilpotent, there exists a positive integer* m *such that* $a_n^m = 0$. *Then*

   $(g(x) + a_nx^n) \cdot$
   $\left(g(x)^{-1} - a_ng(x)^{-2}x^n + a_n^2g(x)^{-3}x^{2n} - ... + (-1)^{m-1}a_n^{m-1}g(x)^{-(m-1)}x^{(m-1)n}\right) = 1.$

   Thus $f(x)$ *is invertible.*

7. Let $f(x) = x^6 + x^3 + 1$. Show that $f(x)$ is irreducible over $\mathbb{Q}$.

   Solution 26 *Now* $f(x+1) = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3$ *and this is irreducible by Eisenstein with* $p = 3$ *so* $f(x)$ *is irreducible.*

8. Give an example of a primitive polynomial which has no root in $\mathbb{Q}$ but is reducible over $\mathbb{Z}$.

   Solution 27 *Let* $f(x) = x^4 + 2x^2 + 1$.

9. Show that a proper ideal I of a ring R is a maximal ideal if and only if for any ideal A of R either $A \subseteq I$ or $A + I = R$.

   Solution 28 *Suppose* I *is a maximal ideal of* R *and let* A *be any ideal of* R. *If* $A \nsubseteq I$, *then* $A + I$ *is an ideal of* R *such that* $I \subset A + I$. *Since* I *is maximal, it follows that* $A + I = R$.

   Conversely, assume that the proper ideal I *satisfies the given condition. Let* J *be an ideal of* R *such that* $I \subset J$. *Now* $J \nsubseteq I$. *Therefore* $I + J = R$. *But* $I + J = J$. *Thus,* $J = R$. *Hence,* I *is a maximal ideal of* R.

10. Let $f(x) = x^5 + 12x^4 + 9x^2 + 6$. Show that the ideal $I = (f(x))$ is maximal in $\mathbb{Z}[x]$.

    Solution 29 I *is a maximal ideal if we can prove that* $f(x)$ *is an irreducible polynomial in* $\mathbb{Z}[x]$. *Then content of* $f(x)$ *is* 1 *and so it is primitive. By Eisenstein and* $p = 3$ *we see that* $f(x)$ *is irreducible. Thus it is a maximal ideal.*

11. The ring $R = \mathbb{Q}[x] / \langle x^4 - 16 \rangle$ is a direct sum of fields. Describe the fields explicitly and determine how many of each appear as direct summands.

Solution 30 *In $\mathbb{Q}[x]$ the principal ideal generated by $x^4-16 = (x-2)(x+2)(x^2+4)$ is the same as the product of the principal ideals generated by each irreducible factor. By the Chinese Remainder Theorem we have*

$$\frac{\mathbb{Q}[x]}{\langle x-2\rangle\langle x+2\rangle\langle x^2+4\rangle} \cong \frac{\mathbb{Q}[x]}{\langle x-2\rangle} \oplus \frac{\mathbb{Q}[x]}{\langle x+2\rangle} \oplus \frac{\mathbb{Q}[x]}{\langle x^2+4\rangle}/$$

Now $\mathbb{Q}[x]$ is a UFD, hence irreducible elements are prime, and in general, prime elements generate principal prime ideals. Furthermore, $\mathbb{Q}[x]$ is a PID, hence nonzero prime ideals are maximal, and thus each term in the direct sum consists of $\mathbb{Q}[x]$ modulo a maximal ideal; that is, each term is a field. Each such field contains a copy of $\mathbb{Q}$, and thus may be viewed a a vector space over $\mathbb{Q}$; as such, the dimension (or degree) over $\mathbb{Q}$ is the same as the degree of the polynomial that generated the corresponding maximal ideal. In particular, the first two fields are just $\mathbb{Q}$, while the last field is a degree 2 extension of $\mathbb{Q}(i)$. Thus the answer is $\mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(i)$.

12. Let $f : R \to S$ be a homomorphism of commutative rings. Prove that $I \subset S$ is a prime ideal, then $f^{-1}(I)$ is also a prime ideal. Give an example where I is maximal but $f^{-1}(I)$ is not maximal.

Solution 31 *(a) We already show previously that the preimage of any ideal is an ideal. Let I be prime. Let $ab \in f^{-1}(I)$. Then $f(ab) = f(a)f(b) \in I$, so that either $f(a) \in I$ or $f(b) \in I$, and thus either $a \in f^{-1}(I)$ or $b \in f^{-1}(I)$. Therefore $f^{-1}(I)$ is prime.*

(b) $\mathbb{Z}[x] \to \mathbb{Q}[x]$, an injection. Take $\langle x \rangle \in \mathbb{Q}[x]$ but the preimage is not maximal in $\mathbb{Z}[x]$ as it is contained in $\langle 2, x \rangle$.

3 Fields

1. Let E be a field extension of the field F with $[E : F] = p$, where p is a prime. Show that for any element $a \in E \backslash K$ we have $E = K(a)$. Hint: Study the subfields of E.

Solution 32 *Done in review session.*

2. (i) Let F be a field and a, b be members of a field containing F. Suppose that a and b are algebraic of degree m and n over F and $(m, n) = 1$. Show that $[F(a, b) : F] = mn$. (ii) Show this is not necessarily true if $(m, n) \neq 1$.

Solution 33 *(i)* $[F(a):F]=m$ *and* $[F(b):F]=n$.

$[F(a,b):F(a)][F(a):F]=[F(a,b):F]=[F(a,b):F(b)][F(b):F]$.

Thus

$$[F(a,b):F(a)]\,m=[F(a,b):F(b)]\,n.$$

Thus $n|[F(a,b):F(a)]$ *and* $m|[F(a,b):F(b)]$. *As* $(m,n)=1$ *we thus have that* $mn|[F(a,b):F]$. *But also* $[F(a,b):F]\leq mn$ *(why?) and thus we have our result.*

3. Consider the unique factorization domain $F[t]$, where F is a field and t is transcendental over F. Show that the polynomial $x^2+tx+t\in F(t)[x]$ is irreducible over $F(t)$. Also show that $x^2+tx+t\in F(x)[t]$ is irreducible over $F(x)$.

Solution 34 *Now* $t\nmid 1$, $t|t$ *but* $t^2\nmid t$. *Note* t *is prime in* $F[t]$. *Thus,* $x^2+tx+t\in F(t)[x]$ *is irreducible over* $F(t)$ *by Eisenstein. If we consider* x^2+tx+t *as a polynomial in* t *over* $F(x)$, *then* $x^2+tx+t=(x+1)t+x^2$. *It follows that Eisenstein does not apply. However, since* $(x+1)t+x^2$ *is of degree* 1 *in* t, *it is irreducible over* $F(x)$.

4. Find the splitting field for the following polynomials over $\mathbb{Q}$.
(i) x^4+1, (ii) x^6+x^3+1

Solution 35 *(i)* $f(x)=\left(x^2+\sqrt{2}x+1\right)\left(x^2-\sqrt{2}x+1\right)$ *over* $\mathbb{Q}\left(\sqrt{2}\right)$. *Therefore the roots are*

$$\frac{\pm\sqrt{2}\pm i\sqrt{2}}{2}$$

Thus you can show that $f(x)$ *splits over* $\mathbb{Q}\left(\sqrt{2},i\right)$.

(ii) Note that $x^9-1=\left(x^6+x^3+1\right)\left(x^3-1\right)$. *The roots of* x^9-1 *are* $1,\omega,\omega^2,...,\omega^8$ *where* $\omega=e^{2\pi i/9}$ *and* $1,\omega^3,\omega^6$ *are the roots of* x^3-1. *Thus* $\omega,\omega^2,\omega^4,\omega^5,\omega^7,\omega^8$ *are the roots of* x^6+x^3+1. *Therefore* $S=\mathbb{Q}\left(\omega,\omega^2,\omega^4,\omega^5,\omega^7,\omega^8\right)=\mathbb{Q}(\omega)$ *is the splitting field over* $\mathbb{Q}$. *Since* x^6+x^3+1 *is irreducible over* $\mathbb{Q}$, $[S:\mathbb{Q}]=6$.

5. Find a splitting field S of x^4-10x^2+21 over $\mathbb{Q}$. Find $[S:\mathbb{Q}]$ and a basis for the splitting field over $\mathbb{Q}$.

Solution 36 $f(x)=\left(x^2-3\right)\left(x^2-7\right)$. *So* $S=\mathbb{Q}\left(\sqrt{2},\sqrt{7}\right)$. *Thus* $[S:\mathbb{Q}]=4$ *and a basis is* $\left\{1,\sqrt{2},\sqrt{7},\sqrt{14}\right\}$

6. If F is a field with a finite number of element, prove that F is not algebraically closed.

Solution 37

7. Let $f(x) = x^n - 1 \in \mathbb{Q}[x]$. Show that the Galois group of $f(x)$ over $\mathbb{Q}$ is commutative.

Solution 38 *Let $\omega = e^{2\pi i/n}$. Then the roots of $f(x)$ are $1, \omega, ..., \omega^{n-1}$. Clearly $K = \mathbb{Q}(\omega)$ is a splitting field of $f(x)$. Let $\alpha, \beta \in Gal(K/\mathbb{Q})$. Now $\alpha(\omega)$ and $\beta(\omega)$ are roots of $f(x)$. Hence, $\alpha(\omega) = \omega^k$ and $\beta(\omega) = \omega^j$ for some k, j; $1 \leq j, k \leq n-1$. Now $(\alpha \circ \beta)(\omega) = \omega^{kj} = (\beta \circ \alpha)(\omega)$. Let $y \in K$. Then $y = \sum_{l=0}^{n-1} a_l \omega^l$ for some $a_l \in \mathbb{Q}$, $1 \leq l \leq n$. Now $(\alpha \circ \beta)(y) = (\alpha \circ \beta)\left(\sum_{l=0}^{n-1} a_l \omega^{kjl}\right)$. Similarly, $(\beta \circ \alpha)(y) = \sum_{l=0}^{n-1} a_l \omega^{jkl}$. Therefore, $\alpha \circ \beta = \beta \circ \alpha$. Thus $Gal(K/\mathbb{Q})$ is abelian.*

8. Find all proper subfields of $\mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}, i\right)$.

Solution 39 *Did in Review session*

9. Show that the Galois group of $f(x) = x^3 - 5$ over $\mathbb{Q}$ is isomorphic to S_3.

Solution 40 *The polynomial is irreducible (Eisenstein) and has a splitting field of $\mathbb{Q}\left(\sqrt[3]{5}, e^{2\pi i/3}\right)$ and is a degree six extension. Thus as the Galois group is a subgroup of S_3 it must be S_3.*