1. (10 points, 5 each.) Find the following.

(a) $((1,2,3)(3,4,2))^{25}$ in S_5, written as a product of disjoint cycles.

Answer: $(1,2)(3,4)$

(b) The monic generator of the ideal of $\mathbb{Q}[x]$ generated by the set $\{x+1,\ x^2+1,\ x^3+1\}$.

Answer: 1.

2. (24 points, 6 points each) Complete the following definitions. You may use, without defining them, any terms or symbols that our text defines before defining the word or symbol asked for. Your definitions do not have to have exactly the same wording as those in the text, but for full credit they should be clear, and mean the same thing as those definitions.

(a) If A is a subset of a group G, then the *normalizer* $N_G(A)$ of A in G means

Answer: $\{g \in G \mid gAg^{-1} = A\}$.

(b) If G is a finite group of order n, and p is a prime, then a *Sylow p-subgroup* of G means

Answer: a subgroup P of G whose order is the largest power of p dividing n.

(c) An integral domain R is called a *unique factorization domain* if for every nonzero nonunit $r \in R$, one can write $r = p_1 \dots p_n$, where n is a positive integer, $p_1, \dots, p_n$ are

Answer: irreducible elements of R

and where, for any other factorization $r = q_1 \dots q_m$ satisfying the conditions filled in above, one has

Answer: $m = n$, and there is a renumbering of the factors such that p_i is an associate of q_i for $i = 1, \dots, n$.

(d) If K is an extension of a field F, then the *degree* of K over F, written $[K:F]$, denotes

Answer: the dimension of K as a vector space over F.

3. (24 points, 6 points each.) For each of the items listed below, either *give an example* with the property stated, or give a brief reason why *no such example exists.*

If you give an example, you are *not* asked to prove that it has the property stated; however, your examples should be specific; i.e., even if there are many objects of a given sort, you should name a particular one. If you give a reason why no example exists, don't worry about giving reasons for your reasons; a simple statement will suffice.

(a) A group homomorphism $\varphi: G \to H$ and a normal subgroup $N \trianglelefteq G$ such that $\varphi(N)$ is not normal in H.

Answer (one of many): $H = S_3$, $G =$ the subgroup $\langle (1,2) \rangle$ of H, and $N = G$, with φ the inclusion homomorphism (sending each element of G to itself in H).

(b) A finite group G which cannot be written as a homomorphic image of any free group.

Answer: Does not exist. If $G = \{g_1, \dots, g_n\}$, let F be a free group on a set of n elements, $\{x_1, \dots, x_n\}$. By the universal property of the free group F, there exists a homomorphism $F \to G$ taking each x_i to g_i, and this will carry F onto G, making G a homomorphic image of F. (There was no real need to assume G finite; I did so just in case your idea of a free group was limited to the case of finitely many generators, since we visited free groups only briefly.)

(c) A ring R and two distinct subsets $A \neq B$ of R, which generate the same ideal, $(A) = (B)$.

Answer (one of many): $R = \mathbb{Z}$, $A = \{1\}$, $B = \{1, 2\}$.

(d) A proper subfield of $\mathbb{Q}$ (i.e., a subfield F of $\mathbb{Q}$ which is not all of $\mathbb{Q}$).

Answer: Does not exist. Any subfield of $\mathbb{Q}$ will contain 1, hence will contain the field it generates, which is all of $\mathbb{Q}$.

4. (12 points) Suppose R is an integral domain which is *not* a principal ideal domain. Show that R has a non-principal ideal A which is *maximal* among non-principal ideals of R; i.e., such that all ideals of R properly containing A are principal. (Recall that a principal ideal of R is an ideal generated by a single element.)

Be detailed in justifying your ring-theoretic assertions. However, you may use the criterion that a subset A of a commutative ring R with 1 is an ideal if and only if it is nonempty, and for all $a, b \in A$ and $r, s \in R$, one has $ra + sb \in A$.

Answer: Let P be the set of all non-principal ideals of R, partially ordered by inclusion. Since R is a domain but not a principal ideal domain, it has non-principal ideals, so P is nonempty. Let us now show that if $\{A_i \mid i \in I\}$ is a nonempty chain of nonprincipal ideals, then their union $A = \cup_{i \in I} A_i$ is also a nonprincipal ideal, and hence gives an upper bound to that chain in P.

We must first show that A is an ideal. Since it contains each of the ideals A_i, it is nonempty. Now suppose $a, b \in A$ and $r, s \in R$. Then $a \in A_{i_0}$, $b \in A_{i_1}$ for some $i_0, i_1 \in I$. Since $\{A_i\}$ is a chain, one of the ideals A_{i_0}, A_{i_1} contains the other; hence it contains both a and b, so being an ideal, it contains $ra + sb$; hence the union A also contains that element.

Thus, A is an ideal. I now claim that it cannot be a principal ideal (a). Indeed, if it were, then since it would contain the generator a, at least one of the ideals A_i in our chain would contain a, hence A_i would contain $(a) = A$, hence would equal A, contradicting the assumption that A_i was nonprincipal.

(*The above concerned a nonempty chain. Strictly speaking, since the book's statement of Zorn's Lemma does not restrict itself to nonempty chains, we also need to verify that the* empty *chain has an upper bound in P. Such a bound will be given by any element of P. But I won't deduct points if you don't note this fact, as long as you have verified as in the first paragraph above that P is nonempty, as is explicitly required by the book's statement of Zorn's Lemma.*)

Zorn's Lemma now tells us that P has a maximal element A, i.e., a nonprincipal ideal maximal among nonprincipal ideals, as desired.

5. (10 points) Below you are to prove three statements. In proving later ones, you may assume the one(s) before it, whether or not you succeeded in proving them.

(a) (2 points) Suppose $\langle r \rangle$ is a cyclic group, written multiplicatively, and s, t are elements of $\langle r \rangle$ that are not squares (elements of the form x^2) in $\langle r \rangle$. Show that st^{-1} is a square in $\langle r \rangle$.

Answer: Let $s = r^m$, $t = r^n$. If m or n were even, then s or t would be a square, $r^{2k} = (r^k)^2$, so they are both odd. Hence $m - n$ is even, so $st^{-1} = r^{m-n}$ is an even power of r, hence is a square.

(b) (4 points) Suppose $F \subseteq K$ are fields, r is an element of the multiplicative group $F^\times$, and s, t are elements of $\langle r \rangle$ (i.e., powers of r in F), neither of which has a square root in F, but each of which has a square root in K: $s = \alpha^2$, $t = \beta^2$ $(\alpha, \beta \in K)$. Show that the two subfields $F(\alpha)$ and $F(\beta)$ of K are equal.

Answer: Since s and t are not squares in $F^\times$, they are not squares in the cyclic subgroup $\langle r \rangle$, so by part (a), *st^{-1} is a square in $\langle r \rangle$, say $st^{-1} = c^2$. Then $(\alpha\beta^{-1})^2 = st^{-1} = c^2$, so $\alpha\beta^{-1} = \pm c$. Thus, we can write $\alpha = \pm c\beta$ and $\beta = \pm c^{-1}\alpha$, from which we can see that $\alpha \in F(\beta)$ and $\beta \in F(\alpha)$. Thus $F(\beta)$ contains F and α, so it contains $F(\alpha)$, and by the same reasoning, $F(\alpha)$ contains $F(\beta)$, so $F(\alpha) = F(\beta)$.*

(c) (4 points) Show that if F is a *finite* field of odd characteristic, and K is any extension field of F, then K has at most one subfield containing F and having degree 2 over F. (Hint: It was proved in the text that every extension of degree 2 of a field F not of characteristic 2 is gotten by adjoining to F the square root of some element of F. This – and another fact from the readings – will allow you to apply part (b) above to such subfields.)

Answer: Consider any two subfields of K containing F and having degree 2 over it. By the fact quoted, we can write these $F(\alpha)$ and $F(\beta)$, where α and β are square roots of elements of F; say $\alpha^2 = s$, $\beta^2 = t$. Since $F(\alpha)$ has degree 2 over F, it is not equal to F, so α does not itself belong to F, and hence neither does $-\alpha$. Since s cannot have more than the two square roots $\pm\alpha$ in K, it is not a square in F; and the same reasoning applies to β.

But we saw in the text that the multiplicative group of every finite field is cyclic; say $F^\times = \langle r \rangle$. Thus, by the preceding paragraph, s and t are elements of $\langle r \rangle$ which are not squares in F, so by part (b), *$F(\alpha) = F(\beta)$, showing that K does not contain two distinct extensions of F of degree* 2.

6. (20 points) One of the simplest of the irreducibility criteria for polynomials that we have learned is that if $f(x) \in \mathbb{Z}[x]$ is monic, and if for some prime number p, the image of $f(x)$ in $\mathbb{F}_p[x]$ is irreducible, then $f(x)$ is also irreducible. (Recall that $\mathbb{F}_p$ denotes $\mathbb{Z}/p\mathbb{Z}$, the field of p elements.)

The six-step argument below, however, will show that the converse is false; i.e., that there are monic irreducible polynomials whose irreducibility cannot be established in that way.

In proving each step below, you may assume the ones before it, whether or not you succeeded in proving them. (But don't expect each to depend precisely on the one before, as in the preceding question.)

(a) (4 points) Show that $x^4 + 1$ is irreducible in $\mathbb{Z}[x]$. (Suggestion: apply Eisenstein's criterion after a change of variable. If you do so, you don't need to justify that method, as I did in class, but you should make clear how the conditions of Eisenstein's criterion are satisfied.)

Answer: Writing $f(x) = x^4 + 1$, we have $f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$. Here every coefficient after the coefficient of the leading term is divisible by the prime 2, and the constant term 2 is not divisible by the square of that prime, so by Eisenstein's Irreducibility Criterion, $f(x+1)$ is irreducible. Hence $f(x)$ is irreducible.

The remaining steps will be devoted to showing, however, that for every prime p, the polynomial $x^4 + 1$ in $\mathbb{F}_p[x]$ is *reducible*. The general method we will use applies to odd primes, so the next part asks you to verify the case $p = 2$ by hand.

(b) (2 points) Show that the polynomial $x^4 + 1 \in \mathbb{F}_2[x]$ is reducible.

Answer: It has 1 as a root. (*In fact, $x^4 + 1 = (x^2 + 1)^2 = (x + 1)^4$ in $\mathbb{F}_2[x]$.*)

We will now develop some facts about extension fields containing roots of $x^4 + 1$, which will lead to a proof of the reducibility of that polynomial in $\mathbb{F}_p$ for all odd primes p.

(c) (4 points) Show that if the polynomial $x^4 + 1$ is irreducible over a field F not of characteristic 2, and if α is a root of that polynomial in an extension field K of F, then α has order exactly 8 in the multiplicative group $K^\times$. (Suggestion: Say why $\{1, \alpha, \alpha^2, \alpha^3\}$ is a basis of $F(\alpha)$ over F, and get the desired conclusion by expressing certain powers of α in terms of that basis. Make clear where you use the fact that the characteristic of F is not 2.)

Answer: If $x^4 + 1$ is irreducible, then since its degree is 4, *a basis for $F(\alpha)$ over F is given by the four elements 1, α, α^2, α^3. The equation $\alpha^4 + 1 = 0$ shows that $\alpha^4 = -1$, so the first* 8 *powers of α, i.e., α, α^2, α^3, α^4, α^5, α^6, α^7, α^8, are α, α^2, α^3, -1, $-\alpha$, $-\alpha^2$, $-\alpha^3$, 1. These* 8 *expressions are linear combinations of 1, α, α^2, α^3, hence are the unique expressions for our elements in terms of that basis; and since F has characteristic not 2, we have $-1 \neq 1$, so none of them before α^8 equals* 1, *so* 8 *is the order of α.*

(d) (4 points) In the situation of part (c), show that the field $F(\alpha)$ has automorphisms φ_3 and φ_5 such that $\varphi_3(\alpha) = \alpha^3$ and $\varphi_5(\alpha) = \alpha^5$, and which both satisfy $\varphi_i(r) = r$ for all $r \in F$.

Answer: Note that $(\alpha^3)^4 = (\alpha^4)^3 = (-1)^3 = -1$, *and similarly* $(\alpha^5)^4 = -1$, *so* α^3 *and* α^5 *are roots in* K *of the irreducible polynomial* $x^4 + 1$ *over* F. *Hence by a result in the text* (*Theorem 8 on p.519, but you don't have to quote it by number*), *there are isomorphisms* $\varphi_3 \colon F(\alpha) \to F(\alpha^3)$ *and* $\varphi_5 \colon F(\alpha) \to F(\alpha^5)$ *which fix all elements of* F, *and carry* α *to* α^3, *respectively* α^5. *Moreover, since* α^3 *and* α^5 *are odd powers of* α, *they are generators of the cyclic group of order* 8, $\langle \alpha \rangle$, *so the fields* $F(\alpha^3)$ *and* $F(\alpha^5)$ *contain* α, *and so are all of* $F(\alpha)$, *so these isomorphisms are actually automorphisms of that field.*

(e) (3 points) In the situation of the preceding part, show that

$$\varphi_3(\alpha + \alpha^3) = \alpha + \alpha^3, \quad \varphi_3(\alpha^2) \neq \alpha^2, \quad \varphi_5(\alpha + \alpha^3) \neq \alpha + \alpha^3, \quad \varphi_5(\alpha^2) = \alpha^2.$$

Answer: Using the relations $\alpha^4 = -1$ *and* $\alpha^8 = 1$, *we see that*

$$\varphi_3(\alpha + \alpha^3) = \alpha^3 + \alpha^9 = \alpha^3 + \alpha, \quad \varphi_3(\alpha^2) = \alpha^6 = \alpha^4\alpha^2 = -\alpha^2,$$

$$\varphi_5(\alpha + \alpha^3) = \alpha^5 + \alpha^{15} = -\alpha - \alpha^3, \quad \varphi_5(\alpha^2) = \alpha^{10} = \alpha^8\alpha^2 = \alpha^2.$$

These satisfy the asserted equalities and nonequalities.

(f) (3 points) In the situation of parts (c)-(e), deduce that the subfields $\{r \in F(\alpha) \mid \varphi_3(r) = r\}$ and $\{r \in F(\alpha) \mid \varphi_5(r) = r\}$ of K are distinct extensions of F, both having degree 2 over F. You may assume without showing the computations that for any automorphism φ of a field K, the set $\{r \in K \mid \varphi(r) = r\}$ is indeed a subfield of K.

Conclude, using the result of the last part of Question 5 (which you may assume whether or not you succeeded in proving it), that $x^4 + 1$ is not irreducible in $\mathbb{F}_p[x]$ for any odd prime p.

Answer: By the equalities and nonequalities of part (e) *above, the subfields of elements not moved by* φ_3, *respectively not moved by* φ_5, *are strictly smaller than* $F(\alpha)$ *and strictly larger than* F, *so their degrees over* F *must be proper divisors of* $[F(\alpha) : F] = 4$ *and must be larger than* 1. *Hence these degrees must both be* 2. *Part* (e) *also showed that each of these subfields contains an element that the other does not, hence they are distinct.*

Part (c) *of Question* 5 *showed that distinct extensions of* F *of degree* 2 *cannot exist within a common extension when* F *is of the form* $\mathbb{F}_p$ *for* p *odd. But if* $x^4 + 1$ *were irreducible in* $\mathbb{F}_p[x]$, *then* $\mathbb{F}_p[x]/(x^4 + 1)$ *would be an extension field of* $\mathbb{F}_p$ *with the properties of parts* (c)-(d) *above; hence it cannot be irreducible.*

(*Though I didn't ask you to prove this, we can immediately deduce from* (b) *and* (f) *that* $x^4 + 1$ *is reducible over* every *field of nonzero characteristic, since every such field has a prime subfield isomorphic to* $F = \mathbb{F}_p$ *for some* p.)

I HOPE YOU DID WELL!

Good luck on your remaining exams, if any
and
HAVE A GOOD VACATION!