SF2729 GROUPS AND RINGS
Final Exam
Wednesday, August 15, 2012

Time: 14:00–18:00
Allowed aids: none
Examiners: Wojciech Chachólski and Carel Faber

Present your solutions to the problems in such a way that the arguments and calculations are easy to follow. Provide detailed arguments to your answers. An answer without explanation will be given no points.

For Problem 1, the final score equals at least the number of points obtained from the homeworks of the groups part of the course. If your solution to Problem 1 is worth more points, then this will be your final score.

For Problem 2, the final score equals at least the number of points obtained from the homeworks of the rings part of the course. If your solution to Problem 2 is worth more points, then this will be your final score.

For each problem, the maximum score is 6 points.

The minimum requirements for the various grades are according to the following table:

Grade	**A**	**B**	**C**	**D**	**E**
Total credit	30	27	24	21	18

Problem 1

(6 points). Let G be a finite group whose order is odd (not divisible by 2). Let H be a subgroup of G of index 3. Prove that H is a normal subgroup of G. (Suggestion: consider the action of G on the set of cosets G/H and the induced homomorphism $G \to S_3$).

Solution

Consider the action of G on the 3-element set of cosets $G/H = \{H, aH, bH\}$. This action induces a homomorphism $\phi : G \to S_3$. By definition, for g in G, $\phi(g)$ is a permutation of $G/H = \{H, aH, bH\}$ given by $H \mapsto gH$, $aH \mapsto gaH$, and $bH \mapsto gbH$. In particular, if g belongs to Ker(ϕ), then $H = gH$ and hence $g \in H$. It follows that Ker(ϕ) $\subset H$ and consequently ϕ is not the trivial homomorphism. Since G has odd order, the image of ϕ can not contain an element of order 2. It follows that the image of ϕ has order 3. Consequently, the index of Ker(ϕ) in G is 3 and therefore $H =$ Ker(ϕ). This shows that H is a normal subgroup.

Problem 2

a. **(4 points)**. Determine a factorization of $g(X) = 4X^3 + 2X^2 - 2X + 6$ into a product of a finite number of irreducibles in each of the following rings:

$$\mathbb{Z}[X], \quad \mathbb{Q}[X], \quad \mathbb{Z}_3[X], \quad \mathbb{Z}_5[X], \quad \mathbb{Z}_7[X].$$

b. **(2 points)**. Determine the prime numbers p for which $g(X)$ factors as a product of 3 linear factors in $\mathbb{Z}_p[X]$.

Solution

a. Note that $g(X) = 2f(X)$, with $f(X) = 2X^3 + X^2 - X + 3$. The factor 2 is an irreducible in $\mathbb{Z}[X]$, but it is a unit in each of the other rings. So let us study $f(X)$. It is primitive in $\mathbb{Z}[X]$, so it is irreducible in $\mathbb{Q}[X]$ if and only if it is irreducible in $\mathbb{Z}[X]$. Since $f(X)$ has degree 3, it is reducible in $\mathbb{Q}[X]$ if and only if it has a zero in $\mathbb{Q}$. We know that such a zero must be of the form $\frac{a}{b}$, with a and b relatively prime in $\mathbb{Z}$ and $a|3$ and $b|2$. This leaves the 8 possibilities ± 1, ± 3, $\pm\frac{1}{2}$, and $\pm\frac{3}{2}$. We can of course simply try all 8 possibilities. Alternatively, we can note that the only zero of $f(X)$ in $\mathbb{Z}_5[X]$ is $1 \in \mathbb{Z}_5$, which leaves only 1 and $-\frac{3}{2}$ as possible zeroes in $\mathbb{Q}$. We find that $-\frac{3}{2}$ is the only zero of $f(X)$ in $\mathbb{Q}$. This gives a factor $2X + 3$ in $\mathbb{Z}[X]$; long division gives the remaining factor $X^2 - X + 1$, which is irreducible in $\mathbb{Z}[X]$ (since it has no zeroes in $\mathbb{Z}$).

The only remaining question is whether $X^2 - X + 1$ factors in $\mathbb{Z}_p[X]$ for $p = 3$, 5, or 7. For $p = 3$, we find the factorization $(X + 1)^2$; for $p = 5$, it is irreducible; for $p = 7$, we find the factorization $(X + 2)(X + 4)$.

Answer: in $\mathbb{Z}[X]$, $g(X)$ is the product of the irreducibles 2, $2X + 3$, and $X^2 - X + 1$; in $\mathbb{Q}[X]$, $g(X)$ is the product of the irreducibles $4X + 6$ and $X^2 - X + 1$; in $\mathbb{Z}_3[X]$, $g(X)$ is the product of the irreducibles X, $X+1$, and $X+1$; in $\mathbb{Z}_5[X]$, $g(X)$ is the product of the irreducibles $4X + 6$ and $X^2 - X + 1$; in $\mathbb{Z}_7[X]$, $g(X)$ is the product of the irreducibles $4X + 6$, $X + 2$, and $X + 4$.

b. For $p = 2$, $g(X) = 0$ in $\mathbb{Z}_p[X]$, but for other primes, by the above, the question is whether $X^2 - X + 1$ factors in $\mathbb{Z}_p[X]$. Note that $(X + 1)(X^2 - X + 1) = X^3 + 1$, so a zero α of $X^2 - X + 1$ in $\mathbb{Z}_p$ satisfies $\alpha^3 = -1$, hence $(-\alpha)^3 = 1$. So $-\alpha$ is an element of order dividing 3 in the multiplicative group of $\mathbb{Z}_p$. For $p = 3$, $-\alpha = 1$, but for $p \neq 3$, $-\alpha \neq 1$, so $-\alpha$ has order 3. If $p \equiv 2 \pmod 3$, then $\mathbb{Z}_p^*$, of order $p - 1$, doesn't contain an element of order 3, so $X^2 - X + 1$ is irreducible in $\mathbb{Z}_p[X]$. If $p \equiv 1 \pmod 3$, then $\mathbb{Z}_p^*$ does contain an element of order 3, hence a zero of $X^2 - X + 1$, so $X^2 - X + 1$ is reducible in $\mathbb{Z}_p[X]$.

Answer: $g(X)$ factors as a product of 3 linear factors exactly when $p = 3$ or $p \equiv 1 \pmod 3$.

Problem 3

Let G be a group. An element g in G is called a **simple commutator** if there are elements a and b in G such that $g = aba^{-1}b^{-1}$. The subgroup of G generated by all the simple commutators in G is denoted by $[G, G]$ and called the commutator subgroup of G.

a. **(1 point)**. Is the conjugation of a simple commutator a simple commutator?

b. **(1 point)**. Show that $[G, G]$ is a normal subgroup in G.

c. **(1 point)**. Prove that $G/[G, G]$ is an abelian group.

d. **(1 point)**. Prove that any cycle of length 3 in the permutation group S_5 is a simple commutator.

e. **(2 points)**. Prove that $[A_5, A_5] = A_5$.

Solution

a. The conjugation of a simple commutator is also a simple commutator, since:

$$xaba^{-1}b^{-1}x^{-1} = xax^{-1}xbx^{-1}xa^{-1}x^{-1}xb^{-1}x^{-1} = (xax^{-1})(xbx^{-1})(xax^{-1})^{-1}(xbx^{-1})^{-1}.$$

b. An element of $[G, G]$ can be written as a product of simple commutators and inverses of simple commutators. The conjugation of a simple commutator is a simple commutator. As the conjugation is a group homomorphism, it takes a product of simple commutators and inverses of simple commutators to a product of simple commutators and inverses of simple commutators. It follows that $[G, G]$ is a normal subgroup of G.

c. The group $G/[G, G]$ is abelian, since:

$$a[G, G]b[G, G] = ab[G, G] = baa^{-1}b^{-1}ab[G, G] = ba[G, G] = b[G, G]a[G, G].$$

d. Let a, b, c be different elements of the set $\{1, 2, 3, 4, 5\}$. Note that $(abc) = (ab)(bc)(ab)(bc)$. Consequently, (abc) is a simple commutator.

e. Assume that a, b, c, d, e are different elements of the set $\{1, 2, 3, 4, 5\}$. The cycles (abc) and (abd) in S_5 are even and hence they belong to A_5. Their simple commutator can be calculated as follows:

$$(abc)(abd)(abc)^{-1}(abd)^{-1} = (abc)(abd)(cba)(dba) = (ab)(cd).$$

Thus any element in A_5 of the form $(ab)(cd)$ belongs to $[A_5, A_5]$. Consequently, so does any element of the form $(ab)(cd)(cd)(be) = (ab)(be)$. Since any element in A_5 is a product of elements of the form $(ab)(cd)$ and $(ab)(be)$, we can conclude that $A_5 = [A_5, A_5]$.

Problem 4

a. **(2 points)**. Determine an irreducible polynomial $f(X)$ of degree 2 in $\mathbb{Z}_3[X]$.

b. **(2 points)**. Determine a generator of the multiplicative group of the finite field

$$\mathbb{Z}_3[X]/\langle f(X)\rangle.$$

c. **(2 points)**. Determine all elements of order 5 in the multiplicative group of the finite field $\mathbb{Z}_{31}$.

Solution

a. By counting the monic reducible polynomials of degree 2, one easily finds that there are $\frac{1}{2}p(p-1)$ monic irreducible polynomials of degree 2 in $\mathbb{Z}_p[X]$. For $p = 3$, this gives 6 irreducible polynomials; one easily finds that they are

$$\pm(X^2 + 1), \quad \pm(X^2 + X - 1), \quad \pm(X^2 - X - 1),$$

since none of these has a zero in $\mathbb{Z}_3$. Let us take $f(X) = X^2 + 1$ (which in some sense is the simplest one).

b. Since $f(X)$ is irreducible, $\langle f(X) \rangle$ is a maximal ideal in $\mathbb{Z}_3[X]$, so the quotient is a field F. This field has 9 elements, so its multiplicative group F^* has 8 elements. We know that F^* is cyclic and need to find a generator. Since F^* is cyclic of order 8, an element $\alpha \in F^*$ is a generator if and only if $\alpha^4 \neq 1$. We first try $\alpha = \overline{X} = X + \langle f(X) \rangle$, but this fails, since $\alpha^2 = -1$, so $\alpha^4 = 1$. The 4 elements of order dividing 4 in F^* are therefore 1, -1, $\overline{X}$ and $-\overline{X}$. Any other element $\pm\overline{X} \pm 1$ will do.

c. Analogously, the multiplicative group of $\mathbb{Z}_{31}$ is a cyclic group G of order 30. If g is a generator, then g^6 has order 5 and generates the subgroup of elements of order dividing 5; note that this subgroup is a cyclic group of order 5. So we are looking for the nontrivial elements of this subgroup; and any such element will generate it, since 5 is prime. Now we note that $2^5 = 32 = 1$ in $\mathbb{Z}_{31}$, so $2 \in \mathbb{Z}_{31}$ has order 5, and the other elements of order 5 are $2^2 = 4$, $2^3 = 8$, and $2^4 = 16$.

Problem 5

Let S_7 be the permutation group of the set $\{1, 2, 3, \ldots, 7\}$.

a. **(1 point)**. Is there a simple commutator in S_7 (see Problem 3) which is an odd permutation?

b. **(3 points)**. Find the number of different elements of order 7 in S_7.

c. **(2 points)**. Find the maximal order of a cyclic subgroup of S_7.

Solution

a. A simple commutator is always an even permutation. Here is why. Consider a simple commutator $aba^{-1}b^{-1}$. Assume that a can be written as a product of k transpositions and b can be written as a product of l transpositions. The inverses a^{-1} and b^{-1} can then be written as products of respectively k and l transpositions. Consequently the simple commutator $aba^{-1}b^{-1}$ can be written as a product of $2k + 2l$ transpositions, which is an even number of transpositions.

b. Any element in S_7 can be written as a product of disjoint cycles. The order of such an element is then the least common multiple of the lengths of the cycles occurring in the product. Since 7 is a prime, it follows that the only permutations in S_7 of order 7 are cycles of length 7. Any such cycle can be uniquely written in the form $(1abcdef)$ where a, b, c, d, e, f can be arbitrary distinct elements in the set $\{2, 3, 4, 5, 6, 7\}$. The number of such permutations is therefore given by the product $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 = 720$.

c. As before, any element in S_7 can be written as a product of disjoint cycles. The order of such an element is then the least common multiple of the lengths of the cycles occurring in the product. Let τ be an arbitrary permutation in S_7. Write it as a product of disjoint cycles $\tau = c_1 c_2 \cdots c_k$. We call the sequence of numbers $[|c_1|, |c_2|, \ldots, |c_k|]$ the cycle type of τ.

- If one of the cycles has order 7 or 6, then the cycle type of τ can be either $[7]$ or $[6]$. Thus τ has order 7 or 6.
- If one of the cycles has order 5, then the cycle type of τ can be either $[5]$ or $[5, 2]$. Consequently, the order of τ is either 5 or 10.
- If one of the cycles has order 4, then the cycle type of τ can be either $[4]$ or $[4, 2]$ or $[4, 3]$. Consequently, the order of τ can be either 4 or 12.
- If one of the cycles has order 3, then the cycle type of τ can be either $[3]$ or $[3, 2]$, or $[3, 3]$, or $[3, 4]$, or $[3, 2, 2]$. In this case the order of τ is either 3 or 6 or 12.
- If one the cycles has order 2, then the cycle type of τ can be either $[2]$, or $[2, 2]$, or $[2, 3]$, or $[2, 4]$, or $[2, 5]$, or $[2, 2, 2]$, or $[2, 2, 3]$. In this case the order of τ is either 2, or 4, or 6, or 10.

We can conclude that the maximal order of a cyclic subgroup of S_7 is 12.

Problem 6

a. **(2 points)**. Denote by K the field $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. Determine the degree of the field extension $K \supset \mathbb{Q}$.

b. **(2 points)**. Determine an element $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$.

c. **(2 points)**. Prove that $p = 13$ is a prime number such that the reductions modulo p of $X^2 - 2$ and of $X^3 - 2$ both are irreducible in $\mathbb{Z}_p[X]$. Is 13 the smallest such prime?

Solution

a. K contains the fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{2})$. The elements $\sqrt{2}$ and $\sqrt[3]{2}$ have irreducible polynomials $X^2 - 2$ respectively $X^3 - 2$ over $\mathbb{Q}$, since these polynomials are irreducible by the Eisenstein criterion. So the fields mentioned have degree 2 respectively 3 over $\mathbb{Q}$. Since $[K : \mathbb{Q}]$ is divisible by these degrees, it is divisible by 6. But $[K : \mathbb{Q}]$ is also at most 6, since K is obtained from $\mathbb{Q}(\sqrt{2})$ by an extension of degree at most 3. We find that $[K : \mathbb{Q}] = 6$ (and hence $X^3 - 2$ remains irreducible over $\mathbb{Q}(\sqrt{2})$).

b. Such an element α will necessarily be of degree 6 over $\mathbb{Q}$. A moment of inspiration will seduce us to try $\alpha = \sqrt[6]{2}$, with irreducible polynomial $X^6 - 2$ over $\mathbb{Q}$ (Eisenstein again). But why would α be an element of K? Observe that $(\sqrt{2})^6 = 2^3$ and $(\sqrt[3]{2})^6 = 2^2$, so that

$$\alpha = \sqrt[6]{2} = \frac{\sqrt{2}}{\sqrt[3]{2}}\,,$$

which shows that $\alpha \in K$.

c. We need to show that 2 is neither a square nor a cube in $\mathbb{Z}_{13}$. The nonzero squares modulo 13 are 1, 4, 9, 3, 12, and 10 (of course there are six of them). Similarly, in the multiplicative group $\mathbb{Z}_{13}^*$, cyclic of order 12, there are four cubes, forming a cyclic subgroup of order four. They are 1, -1, 8 and $-8 = 5$. This proves that both $X^2 - 2$ and $X^3 - 2$ are irreducible in $\mathbb{Z}_{13}[X]$.

In fact, it is easy to see that 13 is the smallest prime p as in the problem ($2 = 0$ modulo 2, $2 = (-1)^3$ modulo 3, $2 = 3^3$ modulo 5, $2 = 3^2$ modulo 7, and all elements of $\mathbb{Z}_{11}^*$ are cubes).