Math. 553 Final Exam—Solutions Dec. 14, 2011

Please begin your solution to each problem 1–5 on a new sheet.

When answering any part of a problem you may assume you have done the preceding parts.

Notation: $\mathbb{Z}$ (*resp.* $\mathbb{Q}$) *is the ring of rational integers* (*resp. the field of rational numbers*).

---

1. Let G be a group of order 105.

(a) Show that G has a normal subgroup of order 5 or 7. `[points]:[4]`

(b) Show that G has a cyclic normal subgroup of order 35. `[4]`

(c) Show that the Sylow 5- and 7-subgroups of G are *both* normal. `[3]`

(d) Classify groups of order 105. `[4]`

Solution. (a) If a Sylow 5-subgroup F is not normal, then it has $1+5k$ conjugates where $k \geq 1$ and $1+5k$ divides $105/5 = 21$, whence $1+5k = 21$ and there are $21 \cdot 4 = 84$ elements of order 5. Similarly if a Sylow 7-subgroup S is not normal, then there are $15 \cdot 6 = 90$ elements of order 7. Since $84 + 90 > 105$, at least one of F and S must be normal.

(b) Since at least one of F and S is normal, and (clearly) $|F \cap S| = 1$, therefore $FS < G$ is a subgroup of order 35. Since 5 doesn't divide $7-1$, every group of order 35 is cyclic.

(c) The cyclic group FS has unique subgroups of orders 5 and 7, so it has 31 elements of order $\neq 5$, and 29 elements of order $\neq 7$. Hence, and since $|G| = 105$, G cannot have 84 elements of order 5 or 90 of order 7; so by the proof of (a), both F and S are normal.

(d) As in (b), if T is the Sylow 3-subgroup, then, since $S \triangleleft G$, therefore $TS < G$ is a subgroup of order 21, a complement of $F \triangleleft G$. Since $|\mathrm{Aut}(F)| = 4$, any homomorphism $TS \to \mathrm{Aut}(F)$ is trivial; and consequently G is the direct product $TS \times F$. There are, up to isomorphism, just two groups of order 21, and one of order 5; correspondingly, there are just two possibilities for G.

---

2. Let $n > 1$ be in $\mathbb{Z}$, and let $R := \mathbb{Z}[\sqrt{-n}\,]$.

For $x = a + b\sqrt{-n} \in R$ $(a, b \in \mathbb{Z})$, set $\bar{x} = a - b\sqrt{-n}$, and define the norm

$$N(x) = x\bar{x} = a^2 + nb^2.$$

(a) Assuming $x \neq 0$, describe group isomorphisms $R/xR \cong R/\bar{x}R \cong xR/x\bar{x}R$. `[4]`

(b) Deduce from (a) that $N(x)^2 = [R : xR][xR : x\bar{x}R] = [R : xR]^2$. `[3]`

(c) Deduce from (b) that if $N(x)$ is prime in $\mathbb{Z}$ then x is prime in R. `[4]`

(d) Deduce from (c) that if p is a prime in $\mathbb{Z}$ then there is *at most one* way to represent p in the form $p = a^2 + nb^2$ where a and b are positive integers. `[4]`

Solution. (a) The automorphism of R that takes any $y \in R$ to $\bar{y}$ induces the first isomorphism. Multiplication by x induces the second (which is clearly surjective, and also injective since if $xy = x\bar{x}z$ then, R being an integral domain, $y = \bar{x}z$).

(b) Taking $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ to $a + b\sqrt{-n} \in R$ gives a group isomorphism. For $n > 0 \in \mathbb{Z}$, there results an isomorphism $\mathbb{Z}_n \times \mathbb{Z}_n \cong R/nR$; so the cardinality $|R/nR| = [R : nR] = n^2$. In particular, for $n = x\bar{x}$ one gets $N(x)^2 = [R : x\bar{x}R] = [R : xR][xR : x\bar{x}R] = [R : xR]^2$, where the last equality holds by (a).

(c) If $N(x) \overset{\text{(b)}}{=} |R/xR|$ is prime, so that R/xR has no nontrivial proper subgroup, then the ideal xR is maximal, hence prime, i.e., x is prime in R.

(d) By (c), if $p = a^2 + nb^2 = x\bar{x}$ ($x := a + b\sqrt{-n}$) is a $\mathbb{Z}$-prime then $p = x\bar{x}$ is a factorization of p into R-primes. By (b), any unit $u + v\sqrt{-n}$ in R has norm ± 1, i.e., $u^2 + nv^2 = \pm 1$, whence $u = \pm 1$ and $v = 0$. Since factorization into primes is unique up to multiplying by units and permuting the factors, it follows that if $p = a^2 + nb^2 = c^2 + nd^2$ with a, b, c and d all positive then $a = c$ and $b = d$.

---

3. (a) Prove that in $\mathbb{Z}[\sqrt{-5}\,]$, 7 is irreducible but not prime. [10]

(b) Is $\mathbb{Z}[\sqrt{-5}\,]$ a Principal Ideal Domain? (Justify your answer.) [5]

Solution. (a) By substituting y for $\bar{x}$ in (a) and (b) of problem 2, one sees that $N(xy) = N(x)N(y)$. (You could also just say this was proved—differently—in class.)

If $7 = xy$ with neither x nor y a unit, then $N(7) = 49 = N(x)N(y)$, and since $N(x) > 1$, $N(y) > 1$ (cf. problem 2), therefore $N(x) = N(y) = 7$. But this can't be, since $a^2 + 5b^2 = 7$ has no integer solution. Thus 7 is irreducible.

On the other hand, 7 divides $(3 + \sqrt{-5}\,)(3 - \sqrt{-5}\,)$ without dividing either factor; so 7 is not prime.

(b) $\mathbb{Z}[\sqrt{-5}\,]$ is *not* a Principal Ideal Domain, because Principal Ideal Domains are Unique Factorization Domains, rings in which irreducible elements are always prime.

---

4. Let K be a finite field of cardinality q, let $n > 0$ be an integer relatively prime to q, and let ζ be a primitive n-th root of unity lying in some field $L \supset K$ with $[L : K] = m$.

(a) Show that n divides $q^m - 1$. [4]

(b) Show that $[K(\zeta) : K]$ is the order of q in the group $(\mathbb{Z}/n\mathbb{Z})^*$ (units in $\mathbb{Z}/n\mathbb{Z}$). [6]

Solution. (a) By the definition of "primitive n-th root of unity," n is the order of ζ in the multiplicative group L^*; so $n \,\big|\, |L^*| = q^m - 1$.

(b) By (a), the order μ of q divides $[K(\zeta) : K]$. So $K(\zeta)$ contains a subfield $L' \supset K$ such that $[L' : K] = \mu$. The cyclic group L'^* has order $q^\mu - 1$ divisible by n, so it contains a cyclic subgroup of order n, and therefore it contains all the n solutions of $X^n - 1$, one of which is ζ, whence $L' = K(\zeta)$ and $[K(\zeta) : K] = [L' : K] = \mu$.

---

5. Let $f(X) = X^6 + aX^3 + 1 \in \mathbb{Z}[X]$ be irreducible, and let $\mathcal{G} \subset S_6$ be its galois group.

(Analyzing possible factorizations, it is not hard to show—but you needn't do so now—that f *is reducible* $\iff$ $a = p^3 - 3p$ *for some* $p \in \mathbb{Z}$.)

Let F be a splitting field of f (over $\mathbb{Q}$).

(a) Show that if $|a| \geq 2$ then f has a real root x, and that with ω a primitive cube root of unity, the other roots are ωx, $\omega^2 x$, $1/x$, ω/x, and ω^2/x. [6]

(b) Show that $\mathcal{G}$ is isomorphic to the order-12 dihedral group D_{12}. [10]

Hint. Show that there is an order-6 automorphism ψ of F with $\psi x = \omega/x$ and $\psi\omega = \omega^2$. Also, complex conjugation gives an automorphism γ of order 2.

(c) For x as in (a), it is easily seen—and you may assume—that $x + 1/x$, $\omega x + 1/(\omega x)$, and $\omega^2 x + 1/(\omega^2 x)$ make up a single $\mathcal{G}$-orbit, and are distinct roots of $X^3 - 3X + a$.

Show that there are precisely three fields $E \subset F$ such that $[E : \mathbb{Q}] = 3$, that these are conjugate to each other, and that each is generated over $\mathbb{Q}$ by a root of $X^3 - 3X + a$. [9]

Total points: [80]

Solution. (a) A real cube root x of $(-1+\sqrt{a^2-4})/2$ is a root of f. It is easy to check that if y is any root of f then ωy, $\omega^2 y$, $1/y$, ω/y, and ω^2/y are also roots. Since $y \neq 0$, therefore $y \neq \omega y$ and $y \neq \omega^2 y$. If $y = \omega^i/y$ $(0 \le i \le 2)$ then $y^3 = 1/y^3$, so $y^3 = \pm 1$, and $y^6 + ay^3 + 1 = 1 \pm a + 1 \neq 0$ because $a = \pm 2 \implies f$ reducible. So $y \neq \omega^i/y$; and as before $y \neq \omega^j y$ $(j = 1, 2)$. Thus the roots are distinct, and (a) results.

(b) By (a), $F = \mathbb{Q}(x, \omega)$; and since x is real and ω is not, and x is a root of a degree-6 irreducible polynomial, therefore

$$|\mathcal{G}| = [F : \mathbb{Q}] = [\mathbb{Q}(x,\omega) : \mathbb{Q}(x)][\mathbb{Q}(x) : \mathbb{Q}] = 2 \cdot 6 = 12.$$

The two automorphisms of $\mathbb{Q}(\omega)$ extend to automorphisms of the splitting field F (shown in class). An extension θ is uniquely determined by $\theta(x)$, which is a root of f, so there are at most six extensions, and there must be exactly six because F has twelve automorphisms. In other words, for each root y of f, there is a θ with $\theta(x) = y$. Thus the nonidentity automorphism of $\mathbb{Q}(\omega)$, which takes ω to ω^2, extends to an automorphism ψ of F with $\psi x = \omega/x$. Then

$$\psi^2(x) = \psi(\omega/x) = \omega^2/(\omega/x) = \omega x \neq x,$$

whence $\psi^4(x) = \omega^2 x$ and $\psi^6(x) = x$. Also $\psi^3(\omega) = \omega^2 \neq \omega$; and $\psi^6(\omega) = \omega$. Hence ψ^6 is the identity, while ψ^2 and ψ^3 are not—that is, ψ has order 6. So ψ generates a cyclic subgroup $\mathcal{C} \subset \mathcal{G}$, which is of index 2 and hence normal.

An easy calculation shows that $\gamma\psi\gamma^{-1} = \psi^{-1}$. (Just apply both sides to x and to ω.) So γ is not contained in $\mathcal{C}$ (which is commutative), and hence generates a complement of $\mathcal{C}$. Thus $\mathcal{G} \cong \mathbb{Z}_2 \rtimes_\phi \mathbb{Z}_6$ where ϕ takes the generator of $\mathbb{Z}_2$ to the automorphism $\xi \mapsto \xi^{-1}$ of $\mathbb{Z}_6$, that is, $\mathcal{G} \cong D_{12}$.

(c) Fields E with $[E : \mathbb{Q}] = 3$ correspond 1-1 to order-4 subgroups of $\mathcal{G} \cong D_{12}$, i.e., to Sylow 2-subgroups, of which there must be 1 or 3. There can't be 1, because, e.g., D_{12} has seven elements of order 2 (as one sees, e.g., by representing D_{12} as a group of symmetries of a regular hexagon), each of which is contained in a Sylow 2-subgroup. So there are 3 subfields of degree 3, conjugate to each other (since that is true for the Sylow 2-subgroups).

The polynomial $X^3 - 3X + a$ is irreducible over $\mathbb{Q}$, because it has the three given $\mathcal{G}$-conjugate roots. So any of these roots generates a degree-3 subfield, whose conjugates are the subfields generated (respectively) by the other two roots. By the preceding paragraph, these must be the three sought-after subfields.

Supplementary exercise. Prove that F has precisely three quadratic subfields, generated by the square roots of -3, $a^2 - 4$ and $(-3)(a^2 - 4)$, respectively.

Which one is the fixed field of $\mathcal{C}$? Which contains the discriminant of f? Of $X^3 - 3X + a$?
